L'ATTUAZIONE DELLA SECONDA DIRETTIVA SUI SERVIZI DI PAGAMENTO E "OPEN BANKING"

—

THE TRANSPOSITION OF PSD2 AND OPEN BANKING

A cura di / (Edd.)
E. Bani, V. De Stasio, A. Sciarrone Alibrandi

BERGAMO UNIVERSITY PRESS
sestante edizioni

CURATORI

Elisabetta Bani è professoressa ordinaria di Diritto dell'Economia e Direttrice del Dipartimento di Giurisprudenza nell'Università degli Studi di Bergamo. Le sue pubblicazioni scientifiche riguardano soprattutto il diritto pubblico dell'economia e il diritto bancario, la vigilanza sui mercati bancari e finanziari, l'impresa sociale e il terzo settore.

Vincenzo De Stasio è professore ordinario di Diritto commerciale nell'Università degli Studi di Bergamo, avvocato in Milano. Ha partecipato ai lavori di riforma del diritto societario nel 2001-2004 ed è stato consigliere di amministrazione indipendente in Banca Infrastrutture Innovazione e Sviluppo e in Banca Imi. Attualmente è consigliere di amministrazione in Fondazione Cariplo.
Le sue pubblicazioni scientifiche riguardano soprattutto il diritto societario, il diritto della cooperazione e della mutualità, il diritto bancario e dei pagamenti.

Antonella Sciarrone Alibrandi è professoressa ordinaria di Diritto dell'Economia e Prorettrice dell'Università Cattolica del Sacro Cuore. Presidente dell'Associazione dei Docenti di Diritto dell'Economia (ADDE). È stata membro del Collegio di Milano dell'Arbitro Bancario Finanziario. Attualmente fa parte del Consiglio dell'Autorità di Supervisione e Informazione Finanziaria della Città del Vaticano. Le sue pubblicazioni scientifiche riguardano il diritto civile, bancario e dei mercati finanziari, con particolare attenzione da oltre venticinque anni al diritto dei pagamenti.

EDITORS

Elisabetta Bani is full professor of Economic Law and Dean of the Department of Law at the University of Bergamo. Her scientific publications mainly concern regulation in economics and banking law, supervision of banking and financial markets, social enterprise and the third sector.

Vincenzo De Stasio is full professor of Commercial Law at the University of Bergamo, a lawyer in Milan. Member of the Government corporate law reform Commission in 2001-2004; former independent director of Banca Infrastrutture Innovazione e Sviluppo and Banca Imi. He is currently a member of the Board of directors of Cariplo Foundation. His scientific publications mainly concern company law, cooperation and mutuality law, banking and payment law.

Antonella Sciarrone Alibrandi is full professor of Economic Law and Vice Rector of the Università Cattolica del Sacro Cuore. President of the Association of Professors of Economic Law (ADDE). She was a member of the Milan Panel of the Banking and Financial Ombudsman. She is currently a member of the Board of the Supervisory and Financial Information Authority of the Vatican City. Her scientific publications concern civil, banking and financial market law, with particular attention for over twenty-five years to the law of payments.

L'ATTUAZIONE DELLA SECONDA DIRETTIVA SUI SERVIZI DI PAGAMENTO E "OPEN BANKING"

—

THE TRANSPOSITION OF PSD2 AND OPEN BANKING

A cura di / (Edd.)
E. Bani, V. De Stasio, A. Sciarrone Alibrandi

BERGAMO UNIVERSITY PRESS
sestante edizioni

Sestante Edizioni - Bergamo
www.sestanteedizioni.it

L'ATTUAZIONE DELLA SECONDA DIRETTIVA
SUI SERVIZI DI PAGAMENTO E "OPEN BANKING"
–
THE TRANSPOSITION
OF PSD2 AND OPEN BANKING

a cura di/(Edd.)
E. Bani, V. De Stasio, A. Sciarrone Alibrandi

p. 236 - cm 15x22

ISBN – 978-88-6642-368-3

In copertina:
Miniatura francese del XV secolo con la scena del pagamento degli affitti.

INDICE
/ CONTENTS

Introduzione pag. 9

Introduction » 17

I PARTE / *FIRST PART*
GLI EFFETTI DELL'ATTUAZIONE DELLA PSD2 SUL MERCATO DEI PAGAMENTI. UN'ANALISI GIURIDICO-ECONOMICA
THE IMPACT OF THE TRANSPOSITION OF PSD2 ON THE MARKET OF PAYMENT SERVICES. LEGAL AND ECONOMIC ISSUES

Alberto Franco Pozzolo
PSD2 and the transformation of the business model of payment services providers » 27

Gustavo Olivieri
PSD2, MIF and Antitrust enforcement in the new markets for online payment services » 43

Robert Freitag
PSD2 and other EU-Directives in the Banking and Financial Sector. The Case of the Directives on Electronic money and on the Distance Marketing of Financial Services » 55

II PARTE / *SECOND PART*
GLI EFFETTI DELL'ATTUAZIONE DELLA PSD2 SULLA TUTELA DEI CLIENTI
THE IMPACT OF THE TRANSPOSITION OF PSD2 ON CUSTOMER PROTECTION

Simone Mezzacapo
PSD2, online and mobile payments: what transparency for the future of payments? » 69

Ugo Minneci
Unauthorized Payment transactions according to PSD 2 enforcement: from the Banking and financial ombudsman to case-law » 109

THIRD PART
THE TRANSPOSITION OF PSD2: THE ROLE OF EBA AND THE NATIONAL RULEMAKERS

Dimitrios Linardatos
The transposition of the PSD 2: the role of EBA and of the national legislator in Germany » 121

Maria Raquel Guimarães
The transposition of PSD2: Decree-Law 91/2018 of 12 November, the Portuguese experience and what may (or may not) change » 141

Reinhard Steennot
Liability for unauthorized payment transactions: the transposition of PSD2 in Belgium » 167

Martin Miernicki
Transposition of the PSD2 in Austria » 189

Thierry Bonneau
The transposition of the PSD2 in France » 207

Vittorio Santoro
Considerazioni conclusive » 217

Concluding remarks » 225

Contributors » 235

INTRODUZIONE

1. Costituisce esperienza comune – ed è anche in questi giorni all'attenzione delle cronache, per effetto della pandemia da COVID-19 – il mutamento delle modalità con cui avvengono i pagamenti nella vita quotidiana. Quando la Banca d'Italia diede avvio, con il Libro bianco sui pagamenti del 1987, a una importante riflessione sulle trasformazioni richieste al sistema dei pagamenti, larga parte dei pagamenti dell'economia italiana avveniva in contanti o con assegni bancari e circolari, cioè con strumenti di pagamento basati su carta.

Il legislatore europeo, le Autorità di vigilanza dell'Unione e nazionali hanno compiuto nei decenni scorsi degli sforzi enormi per rendere il complesso dei servizi e dei sistemi di pagamento sempre più uniforme nello Spazio Economico Europeo. Lo scopo pratico è quello di consentire un utilizzo senza problemi dei servizi di pagamento qualunque sia la localizzazione geografica dell'IBAN di partenza e dell'IBAN di arrivo del pagamento. Un grande aiuto è derivato anche dal settore dell'industria bancaria e dei pagamenti, il cui sforzo di autoregolamentazione e di soluzione dei problemi pratici costituisce una parte ineliminabile del funzionamento, perfetto come quello di un orologio, di strutture che devono accompagnare ogni economia moderna. Banche commerciali, prestatori di servizi di pagamento, sistemi di pagamento, banche centrali, tra loro fortemente interconnessi, risolvono senza posa – e senza sforzo apparente all'esterno – problemi pratici complicatissimi, che vedono al loro

centro la trasmissione di ordini di pagamento e i corrispondenti trasferimenti elettronici di fondi.

Dietro all'uso delle carte di pagamento, delle carte di credito, dei nuovi servizi di disposizione di ordine e di informazione sui conti, così immediato da parte dell'utente, si celano complessi problemi giuridici e tecnologici, la cui soluzione ha consentito di dare rapidità di esecuzione e sicurezza sempre maggiore all'operazione di pagamento. La tecnologia si basa oggi anche su strumenti di intelligenza artificiale e su un uso sempre più massiccio di dati personali, che pongono un problema di confine della nostra disciplina del diritto dei pagamenti con altre aree importanti, quale quella del trattamento dei dati personali.

Oggi, ad es., gli studenti dell'Università di Bergamo possono utilizzare la propria tessera di identificazione come carta di pagamento; l'evoluzione della tecnologia applicata alla finanza (cd. *Fintech*) ha consentito di trasformare gli *smartphone* in strumenti di pagamento; il Governo italiano si propone di ridurre l'uso del contante, mentre alcune banche centrali conducono da anni una riflessione sull'uso delle tecnologie per introdurre una moneta digitale di banca centrale; vi sono sempre nuove iniziative nel campo delle valute virtuali: se, nel 2019, un operatore di *social network* aveva costituito un consorzio di imprese del settore dei pagamenti e delle telecomunicazioni per realizzare una nuova moneta digitale internazionale, ora è notizia di cronaca che la BCE ha aperto una consultazione su una moneta digitale di banca centrale.

Il disegno, intravisto nel secolo scorso da un grande e concreto economista della Banca d'Italia come Tommaso Padoa Schioppa, era quello di arrivare a un'operazione di pagamento elettronico che avesse la stessa rapidità e sicurezza della consegna bilaterale del danaro contante, passando però attraverso un sistema che vede la necessaria collaborazione di almeno un prestatore di servizi di pagamento, normalmente la banca o le banche presso cui sono radicati i conti di pagamento dei clienti, ma oggi anche nuovi operatori, come gli istituti di pagamento, e gli istituti di moneta elettronica.

Tutto ciò ha condotto a una trasformazione del modo di pagare, alla sostituzione del contante con procedure intermediate in cui un ordine di pagamento viene impartito elettronicamente e segue, in esecuzione, un trasferimento di fondi da un IBAN a un altro IBAN. La tecnologia informatica, così pervasiva, costituisce il mezzo onnipresente di questo nuovo ambiente monetario. La moneta non si tocca più, e al suo posto circolano dati informatici, a volte "big data", in procedimenti sempre più complessi e articolati. Le conseguenze a volte sono sconcertanti, come ben sanno i notai che si trovano a dover attestare dei pagamenti avvenuti elettronicamente, senza potere disporre dei documenti cartacei di "quietanza" che il codice civile prevede, ma non sempre gli operatori *on-line* sono disposti a rilasciare.

2. Le difficoltà maggiori che incontra l'armonizzazione del diritto dei pagamenti sono forse legate non alla tecnologia – che sostanzialmente si sviluppa senza tenere conto delle frontiere fisiche, tanto più in un'epoca in cui la rete internet mette in discussione le sovranità nazionali – ma alle peculiarità degli ordinamenti nazionali. Il diritto dei pagamenti è materia nella quale le specificità dei diversi ordinamenti giuridici – la loro storia, il loro diritto delle obbligazioni, dei risarcimenti e delle restituzioni, in una parola: il loro codice civile – pesano enormemente sulle ricostruzioni e sull'inquadramento teorico dell'operazione di pagamento, della sua iniziazione, della sua esecuzione e delle responsabilità connesse. Le direttive sui servizi di pagamento sono direttive di armonizzazione massima, ma le tradizioni giuridiche nazionali e le differenti concezioni dei rapporti di delegazione e trilaterali sono forse l'ostacolo più profondo – proprio perché radicato negli ultimi secoli di storia delle codificazioni – alla vera produzione di un diritto uniforme dei pagamenti.

Nella dottrina giuridica tedesca vi sono ricostruzioni raffinatissime dei rapporti trilaterali e delle restituzioni, su cui si innesta una abbondante e cospicua produzione che ha visto i maggiori civilisti

tedeschi occuparsi dei servizi di pagamento. Ma anche la dottrina commercialistica e bancaristica italiana hanno prodotto nel tempo complesse ricostruzioni a partire dallo studio della delegazione, nell'opera pionieristica di Walter Bigiavi ancora sotto l'impero del codice civile del 1865: e come non ricordare in Italia gli altri studi pionieristici di Gian Franco Campobasso sul bancogiro; di Gustavo Olivieri sui circuiti di compensazione; di Vittorio Santoro sul conto corrente bancario; per non parlare degli altri Paesi, degli studi sui servizi di pagamento della dottrina belga, qui rappresentata da Reinhard Steennot; degli studi sul contratto quadro, dovuti alla studiosa portoghese Maria Raquel Guimaraes; del commentario sui servizi di pagamento dovuto alla scuola austriaca del prof. Arthur Weilinger, qui rappresentata dal Dr. Martin Miernicki; delle soluzioni teoriche e pratiche prodotte dai giuristi francesi, sempre all'avanguardia e qui rappresentati dal collega Thierry Bonneau.

Questo lavoro raccoglie contributi di studiosi europei del diritto della concorrenza e dei servizi di pagamento, che hanno cercato di dialogare intensamente tra loro, superando la barriera linguistica che rende spesso reciprocamente inaccessibili le opere monografiche scritte nelle lingue nazionali, o la giurisprudenza scritta nella lingua nazionale del processo. Confidiamo che questo confronto non resti un'iniziativa isolata, ma contribuisca a sviluppare quelle relazioni tra giuristi della comunità scientifica europea, che si devono parlare in inglese ma anche imparare le rispettive lingue nazionali, per creare una comunità accademica veramente integrata: al momento, e in primo luogo ciò che costituisce il fine specifico di questa pubblicazione per comprendere su quali punti, nonostante la "massima armonizzazione" che è il fine della disciplina europea, sussiste tuttora un grande divario, sia nell'attuazione sia nell'interpretazione. Ed è parso chiaro che sono le clausole generali il tema vero dell'armonizzazione, soprattutto per quanto concerne il tema dei pagamenti non autorizzati, che ha catalizzato una buona parte del dibattito. È un confronto che parte dall'Università e in questa sede resta per il momento circoscritto: anche se vi sono luoghi diversi in cui si studia

o si produce scienza e cultura (i pratici – che l'Università chiama e ascolta e con i quali dialoga – a volte sono più esperti dei professori universitari), è soltanto nella *universitas* che lo studio è strettamente collegato all'ascolto, e ci si può permettere di approfondire un argomento con tutto il tempo che esso davvero richiederebbe. I pratici possono dedicare pochi preziosi minuti del loro tempo, spesso inseguiti dalle regole dell'efficienza economica, alla discussione e alla trasmissione del sapere. È solo nelle Università che questo tempo invece si sospende, e l'*otium* diventa conoscenza.

3. La raccolta di saggi internazionali curata dal Dipartimento di Giurisprudenza dell'Università degli Studi di Bergamo è in particolare dedicata all'attuazione, in Italia e nell'Unione europea, della seconda direttiva sui servizi di pagamento (cd. PSD2: *Second Payment Services Directive*: 2015/2366/UE), entrata in vigore nell'ordinamento unionale in data 13 gennaio 2016, attuata in Italia con il D.lgs. 15 dicembre 2017, n. 218, a sua volta entrato in vigore il 13 gennaio 2018. Dopo l'entrata in vigore e la piena implementazione della disciplina comune in tutti i Paesi dell'Unione, che ha fatto seguito all'applicazione (nel mese di settembre 2019) delle norme tecniche di regolamentazione previste dall'art. 98 della Direttiva –, si è sentita la necessità di una riflessione sul modo in cui la Direttiva è stata attuata in diversi Paesi dell'Unione europea, sul ruolo che hanno avuto le autorità di vigilanza, sulle nuove regole in materia di sicurezza dei pagamenti e di cd. "terze parti" che possono avere accesso ai nostri conti di pagamento, sull'evoluzione della concorrenza nel settore dei pagamenti, tra operatori tradizionali e nuovi operatori del Fintech.

Nell'Unione europea il processo di armonizzazione dei servizi di pagamento si è consolidato più di dieci anni fa, con la Direttiva europea 2007/64/CE, una direttiva di armonizzazione massima strettamente collegata all'attuazione del progetto SEPA, cioè alla creazione di un'Area unica dei pagamenti in Euro. La trasformazione così accompagnata dal legislatore europeo si è attuata su diverse

direttrici: l'incremento della concorrenza tra operatori dei servizi di pagamento, con l'apertura del mercato a soggetti nuovi, diversi dalle banche o dai consolidati operatori del settore delle carte di credito; la predisposizione di regole comuni delle operazioni di pagamento, in termini di armonizzazione massima della disciplina.

Attuata in Italia nel 2010, la prima direttiva sui servizi di pagamento ha dato avvio a un processo di uniformazione europea degli schemi di pagamento, che consente agli utenti dei servizi di pagamento dei diversi Stati membri di fruire di modalità comuni di attuazione dei bonifici o degli addebiti diretti sul proprio conto di pagamento, grazie ai cd. "schemi SEPA", che hanno integrato la legislazione primaria con regole uniformi convenzionali di attuazione.

Oggi la riflessione indotta dalla seconda direttiva (2015/2366/UE) riguarda le nuove modalità di pagamento che si connettono al commercio elettronico, e i nuovi servizi di informazione sui conti di pagamento e di disposizione di ordine, affidati ai nuovi operatori del *Fintech*, che hanno accesso alle informazioni sui conti correnti – tradizionalmente coperte dal segreto bancario – e possono utilizzarle per consentire nuove operazioni di pagamento nella rete Internet, basate su bonifici e non più sull'esclusivo utilizzo della carta di credito. Nuove sfide si pongono al sistema della concorrenza, alle regole sul trattamento dei dati personali, alla comprensione delle regole e alla ripartizione delle responsabilità nelle operazioni di pagamento, alla creazione di un nuovo diritto europeo dei pagamenti, che richiede un dialogo anche tra i giuristi dei diversi Paesi europei.

La presenza di nuovi operatori economici (oggi i cd. "Third Party Providers" o TPP) implica l'apertura di nuovi mercati e di nuove modalità di svolgimento dell'operazione di pagamento, in una dimensione non più nazionale, ma europea e strettamente legata alla rete Internet: problemi, dunque, di diritto della concorrenza, studiati in Italia da economisti e giuristi.

Una piccola osservazione storico-economica può tornare utile nel riflettere sui rapporti tra sistema bancario – sistema dei paga-

menti – e nuovi operatori nei servizi di pagamento: riguarda il modo controintuitivo in cui possono atteggiarsi i rapporti tra *incumbents* e nuovi entranti con riferimento al sistema dei pagamenti.

Le banche hanno iniziato il loro processo di informatizzazione negli anni Sessanta e hanno aggiunto pezzi di sistema al nascere di nuove esigenze, con l'esito di impiegare sistemi che parlano linguaggi diversi e che non rispondono a un progetto unico e razionale. Inoltre, le banche di oggi sono il frutto di molte fusioni di ieri e ognuna delle banche incorporate era gestita con suoi sistemi informatici che, volta a volta, sono stati integrati o i cui dati sono stati traslati nel sistema dell'incorporante, con qualcosa che di solito finisce *lost in translation*.

Il combinato disposto di questi due fatti storici è che i sistemi utilizzati dagli operatori bancari sono più costosi da manutenere di quanto possa essere costoso costruire un nuovo sistema per i nuovi entranti, che vivono in ambienti informatici coerenti e moderni, e quindi probabilmente più efficienti.

Questo per dire che essere un *incumbent* in questo caso non è necessariamente un vantaggio (se è vera la correlazione negativa tra efficienza e costo del servizio).

Dietro all'uso delle carte di pagamento, delle carte di credito, dei nuovi servizi di disposizione di ordine e di informazione sui conti, così immediato da parte dell'utente, si celano complessi problemi giuridici e tecnologici, e sfide sempre più ardue da affrontare.

Elisabetta Bani
Vincenzo De Stasio
Antonella Sciarrone Alibrandi

INTRODUCTION

1. There is no denying the fact that over the years the ways consumers make payments have radically evolved by progressively abandoning the use of cash and relying on the support of technology. It is exactly for such a shift, that is from the real to the virtual world, that payments have not been affected by any of the measures throughout the world put in place to contain the spread of COVID-19 pandemic. In Italy, the beginning of this evolution is marked by an initiative of the Bank of Italy which in 1987 launched a White Paper ("*Libro bianco*") on payments. This was a manifesto with the intention of sparking interest in relation to the ramifications deriving from the changes that were gradually affecting the payments system as a whole. Back then, payments in Italy were, for the most part, made in cash, with cheques or cashier's cheques: that is, with paper payment instruments.

In recent decades, the European legislator, the supervisory authorities of the European Union and the various member States have made remarkable efforts in order to harmonize payment services and payment systems within the European Economic Area as much as possible. And this has been done for a very pragmatic reason: that of enabling payers to freely utilize payment services regardless of the geographical localization of the IBAN either of the payer or the payee. To be sure, the payment services and banking industry have substantially contributed to the success of this goal.

In fact, its ability to self-regulate and solve the various practical problems has been crucial in ensuring the most efficient functioning (quite similar to that of a watch) of the relevant infrastructures that any advanced economy, utilizing modern payment systems, needs. Commercial banks, payment services providers, payment systems and Central Banks are deeply interconnected and finely tuned to deal with very complicated aspects – despite appearing to be simple from the users' perspective –which consist of matching transfers of orders of payments with the relevant and corresponding electronic transfer of funds.

Payment cards, credit cards, payment initiation services and account information services, despite being regarded by users as friendly and easy-to-use, generate serious technical and legal problems. It is the ability of businesses to solve these problems that has led to an increase in the speed and safety of the execution relating to payment transactions. Indeed, technology relies more and more on artificial intelligence and on a massive amount of personal data being gathered. In this sense, the area of payment services shares many aspects relating to other important areas of the law, such as that of personal data management.

Many situations can be offered as an example. Students at the University of Bergamo may utilize their identification card as a payment card. Thanks to Fintech, smartphones may be used as payment instruments. At the legislative policy level it is worth noting that the Italian Government is seriously committed to reducing the usage of cash in payment transactions, whilst some Central Banks have for some time been studying new technologies that support the creation and functioning of "central bank digital currency". In addition, there are always new initiatives in the field of virtual money. In 2019, a well known social network corporation formed a syndicate amongst businesses dealing with payment services and telecommunications to mint a new digital currency at an international level. Simultaneously, the European Central Bank launched a formal consultation about a potential "central bank digital currency".

In fact, this is the scenario that Tommaso Padoa Schioppa, a prominent and pragmatic economist of the Bank of Italy, anticipated many years ago: that of completing an electronic payment transaction with the same level of speed and security as cash but with the cooperation of at least a payment service provider, such as a bank or the bank where the users' payment accounts are held. Certainly, today new intermediaries may well act as payment service provider: for example, payment institutions and Electronic money institutions.

All this has resulted in a new way of making payments and to the replacement of cash with procedures where a payment order is given electronically, being followed by a transfer of funds from one IBAN to another. Technology, in other words, has become pervasive in so far as it is the pivotal, omnipresent element of this new monetary environment. Money has somewhat dematerialized, it is something that we no longer need to touch. Indeed, data relating to, and managed by, information technology, sometimes "big data", circulates. The consequences might be bewildering to many, as is the case for a number of notaries in Italy each time they are required to confirm that a payment has been made electronically but without witnessing any physical receipt of payment: such that the Civil Code requires; however, many of the intermediaries dealing with electronic payments are unable to issue it.

2. In fact, the major obstacles that lie ahead of the harmonization of the regulation concerning the law of payments within the EU are not related to technology – which on the contrary is designed to operate regardless of any geographical borders – but rather to the peculiarities within the various national legislations of member States. The domestic legal framework of each of the different member States – of which we need to consider either very general aspects such as their historical backgrounds or specific elements concerning their contract laws – heavily affects the construction and theoretical characterization of the payment transaction, its

initiation and its execution. Not to mention those profiles relating to the allocation of liabilities amongst the parties involved in the same payment transaction. It is true that EU directives on payment services pursue maximum harmonization, but the specificities of the national legal systems of the various member States as well as the relevant theoretical constructions of the payment transaction (from the perspective of the "delegation" or a "tri-party transaction") are perhaps the most formidable stumbling blocks to a truly uniformed and harmonized European law of payments.

In recent decades, however, legal scholars and researchers have tried to evaluate, *in lieu* of an entirely domestic perspective, a more comprehensive investigation of the various legal aspects of a payment transaction by allowing more latitude for comparative analysis. Some of the most prominent German civil law academics have produced a highly tuned construction of payment transaction as tri-party transaction and of the relevant issues relating to restitutions. Italian commercial and banking academics too have contributed to the characterization of many aspects related to payment transactions with thorough, detailed analysis: prof. Walter Bigiavi with an extended study of delegation; prof. Gian Franco Campobasso with an accurate analysis of the credit transfer; prof. Gustavo Olivieri with an in-deph investigation of the various systems of clearing and settling of (interbank) payments; prof. Vittorio Santoro with an exhaustive study of the banking current account. Also in other EU jurisdictions, the area of the law of payments has greatly benefited from the influential support of academics: this is certainly the case in Belgium, here represented by prof. Reinhard Steennot; in Portugual, thanks to the key contribution of prof. Maria Raquel Guimaraes relating to the frame contract within payment services; in Austria, represented at this symposium by Dr. Martin Miernicki, that here also deserves to be mentioned for the country's Commentary on payment services edited by prof. Arthur Weilinger; and in France, here represented by prof. Thierry Bonneau, in consideration of the brilliant, avant-garde theoretical constructions of its legal scholars.

Special thanks also go to our colleague Stefano Boatto, for the advice given in the revision of a publication which is essentially bilingual.

This publication is the product of several contributions from European scholars and researchers of antitrust and payment services law. They have tried to construe their opinions by engaging themselves in an intense exchange of perspectives, beyond linguistic barriers (something that more often than not makes domestic legal sources such as books and decisions from judicial authorities inaccessible to outsiders). We do believe that this occasion of debate will not remain isolated. We hope that it will contribute to strengthen relationships amongst European academics that of course talk to each other in English but should also speak the different national languages to guarantee a truly profound integration. And more specifically, to better understand with respect to what elements, aspects or issues concerning the law of payments – despite maximum harmonization – is there the need for a closer debate to reach general consensus. One of the aspects of payment services that the debate, promoted by this symposium, has highlighted as something that lies at the heart of this process towards uniformity of the law of payments is that of the general clauses and standards, especially with respect to non-authorized payments. We therefore welcome the fact that not only legal scholars but also practitioners, who more often than not know practical details that can go undetected by the former, have made valuable contributions to this debate.

3. This publication, edited by the Law Department of the University of Bergamo, collects international essays focused on the incorporation-implementation in Italy and across EU member States of the second Directive on payment services (PSD2: *Second Payment Services Directive*: 2015/2366/UE), which came into force on January 13th 2016. In Italy, PSD 2 was incorporated via Leg. Decree December 15th, 2017, No. 218, which came into force on January 13th, 2018. Further to the incorporation of PSD 2 by all European member States – incorporation that followed,

in September 2019, the application of the regulatory technical standards (article 98, PSD 2) – we felt the need for a more general reflection regarding: the way PSD 2 has been incorporated by each of the different EU member States; what role in this process has been played by supervisory authorities; the new rules concerning the security of payment transactions; third parties' rights which are now allowed to access payment accounts; the development and discipline of competition, in the area of payments, amongst incumbents and new Fintech businesses.

Within the European Union, the harmonization of the law on payment services started more than ten years ago with the Directive 2007/64/CE. This Directive of maximum harmonization was strictly linked to the creation of the SEPA, that is of a single area for payments made in Euro. The European legislator has pursued this process of transformation mainly considering: the increase in the level of competition amongst institutions dealing with payment services by granting access to this industry to intermediaries different to that of banks and well-established credit cards companies; a level playing field for payment transactions in conformity with the principle of maximum harmonization.

Incorporated in Italy in 2010, the first Directive on payment services started a European standardization of payment transactions that enable payment services users of the different EU member States to benefit from common rules on completion of bank transfers or direct debit transactions on "own accounts" (and this thanks to the "SEPA format" that completed primary legislation with uniform-contractual rules of application).

The second Directive enables payments to match and therefore to enhance the efficiency of electronic transactions. In addition, it opens up the new market of information services on payment accounts to new Fintech businesses. This is a "game changer" which puts these businesses in charge of the entire trade process. They can now access current accounts once protected by banking secret and use the relevant information in order to maximize their market

position. At the same time, they can attract new online payment transactions, *i.e.* bank transfers, through their channels not those traditional ones controlled by banks and credit card corporations. Hence, new challenges are coming to the surface for both antitrust and data protection laws. At the same time, this new role attributed by the second Directive to these Fintech businesses requires a more effective legal framework with respect to the way liabilities within a payment transaction are regulated. In the end, the second Directive calls for further consideration and reflection for the establishment of an effective, new European payment law. And this is an achievement that requires thorough cooperation amongst the legal scholars of the different European jurisdictions. Indeed, these new Fintech businesses, technically Third Party Providers, operate on a borderless context: that is, from a legal point of view, in a dimension which cannot be linked to a single jurisdiction but must be at least framed from a European perspective.

This scenario leads to fierce competition between traditional incumbents, *i.e.* banks and intermediaries that employ the same business model, and Third Party Providers. Something that could perhaps be better understood when considered from a historical point of view.

Since the 60s of the last century, banks have constantly being evolving their technological structure: but they have gone through this not for contingent market requirements but mainly due to mergers and acquisitions engineered to inflate profits whilst reducing costs. In this context, information technology assets, once set up by one bank, had to be combined with those of a different bank with which the merge was planned. It is evident that this process has severely weakened the technological good will of the entire baking system: as if, in this process, something has been lost in translation.

In consideration of this background, information technology infrastructures used by banks are not only lethargic and inefficient, but also far more expensive than those brand new IT systems that these new Fintech companies can set up.

Therefore, being an incumbent in this context is certainly not of any advantage (particularly, if we give some weight to the correlation between organizational efficiency and cost of service).

This brief overview appears sufficient enough to assume that payment cards, credit cards, payment initiation services and account information services cannot simply be reduced to cutting-edge benefits for consumers as they entail serious, complex legal issues and increasingly difficult challenges.

Elisabetta Bani
Vincenzo De Stasio
Antonella Sciarrone Alibrandi

I PARTE / *FIRST PART*

GLI EFFETTI DELL'ATTUAZIONE DELLA PSD2 SUL MERCATO DEI PAGAMENTI. UN'ANALISI GIURIDICO-ECONOMICA / *THE IMPACT OF THE TRANSPOSITION OF PSD2 ON THE MARKET OF PAYMENT SERVICES. LEGAL AND ECONOMIC ISSUES*

Alberto Franco Pozzolo
(Roma Tre University)

PSD2 AND THE TRANSFORMATION OF THE BUSINESS MODEL OF PAYMENT SERVICES PROVIDERS[1]

1. Introduction

The provision of payment services is one of the most important activities performed by the financial sector.[2] Traditionally, most of these services have been offered by banks, although in the last decades non-bank financial institutions have gained a prominent role in some specific segments, for example in the credit card business. In the past, despite being a relevant source of revenues for banks and other financial intermediaries, payment services provision has ranked relatively low in the interests of policy makers and academics alike, with most of the attention focused on the soundness of the system rather than on its efficiency.

In recent years, this landscape has changed dramatically. The developments in information and communication technologies have made it possible to perform traditional activities more efficiently, and to devise innovative services which were not available before.

[1] I would like to thank Vincenzo de Stasio, Maria Iride Vangelisti and participants at the Conference on "L'attuazione della seconda direttiva sui servizi di pagamento e 'open banking'", Bergamo, 18-19 October 2019 for comments and suggestions. All remaining errors are my own responsibility.

[2] See De Bonis, R. and Vangelisti, M.I. (2019), *La moneta – Dai buoi di Omero ai bitcoin*, il Mulino, for a comprehensive account of the evolution of the payment system.

New players have entered the market, in some cases increasing the degree of competition to the benefit of customers, in other cases exploiting network economies of scale and their better and exclusive know-how to gain significant market power.

Policy makers have reacted to the innovation in the payment industry. In Europe, the first Payment Services Directive,[3] published in 2007, has set the scene, by defining the rights and obligations for a broad spectrum of payment services, such as credit transfers, direct debits and card payments. Moreover, it has set compulsory information requirements, especially on costs. But the market has evolved rapidly, and yet in 2013 the European Commission has published the proposal of a new Directive on payment services, which was eventually published in 2015, and is widely known as Payment System Directive 2 (PSD2).[4]

The PSD2 intervenes extensively in the regulation of many aspects of the payment industry, defining rights and obligations. One of its aims is to foster competition among service providers, as to cut monopoly rents, reduce costs, and improve efficiency.[5] The adoption of the Directive in the various European countries, and the definition of regulations related to its implementation, has taken some time. For this reason, its impact on the industry has not yet fully shown. Nonetheless, while some effects are becoming visible, stronger ones are certainly to be expected in the coming years.

---

[3] 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.

[4] Directive 2015/2366/EU 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.

[5] For a thorough comparison of PSD1 and PSD2, see Sciarrone Alibrandi, A. (2020), *Impostazione sistematica della PSD2*, in Paglietti, C. and Vangelisti, M.I. (eds.), *Innovazioni e regole nei pagamenti digitali: il bilanciamento degli interessi nella PSD2*, RomaTre Press.

The purpose of this chapter is to discuss how some of the innovations introduced by the PSD2 might impact the business model of payment service providers in the coming years, what the effect on the equilibrium in the industry will be, what new risks may emerge, and what actions should be taken to counter possibly undesired outcomes.[6] The Directive has introduced numerous innovations, but the analysis in this chapter will focus mainly on the potential impact of the introduction of three new types of intermediaries, known as Third Party Providers (TPPs): Payment Initiation Service Providers (PISP), Account Information Service Providers (AISP) and Card-Based Payment Instrument Issuers (CBPII).

The rest of the chapter is organized as follows: the next Section briefly describes the activities of the new types of intermediaries that have been introduced by the PSD2. Section 3 describes the main sources of market power in the payment industry. Section 4, the core of the chapter, discusses the possible impact of the PSD2 on the degree of competition in payments. Section 5 argues in favor of some policy interventions and concludes.

2. The new players at the heart of PSD2

The main impact of PSD2 on the market for payment services will most likely be caused by the introduction of three new types of players: Payment Initiation Service Providers (PISP), Account Information Service Providers (AISP) and Card-Based Payment Instrument Issuers (CBPII).[7]

---

[6] See Zeno-Zencovich, V. (2020), *Prefazione*, in Paglietti, C. and Vangelisti, M.I. (eds.), *Innovazioni e regole nei pagamenti digitali: il bilanciamento degli interessi nella PSD2*, RomaTre Press, for an insightful view of the implications of PSD2 for the payment industry.

[7] As is well explained by Porta (2019), *Obiettivi e strumenti della PSD2*, in Maimeiri, M. and Mancini, M. (eds.), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*, Banca d'Italia, Quaderni

With the burgeoning diffusion of online purchases, PISPs are expected to become important players in the payment procedure, because they link the website of the merchant (i.e., the seller of good or service) with the banking platform of the payer. As such, they are responsible for guaranteeing the payee that the payment has been initiated, so that the merchant can safely transfer the good or service purchased, and the operation can be concluded. Aside from crucial issues related to consumer protection and security, the PSD2 requires that any payment service provider (PSP) is permitted to offer payment initiation services, therefore guaranteeing fair competition in the market. To achieve this goal, the Directive posits that PISPs only need the consent of the account holder to access his banking platform, without being required to use any particular business model, or entering into any contractual relationship with the payer's bank. This requires that common and open standards of communication be implemented, according to guidelines that are provided by the European Banking Authority (EBA). In practice, financial intermediaries holding customers' accounts are mandated to make them easily accessible through Application Program Interfaces (APIs). Importantly, PISPs cannot hold accounts in the name of their customers, but their activity is limited to initiating the provision of payment services.

AISPs cover a different part of the market. The increasing number of relationships that corporations and individuals have with banks and other financial intermediaries allows a better management of

---

di ricerca giuridica 87, settembre 2019, customer authentication and the related responsibilities for Payment Services Providers (PSP) are another relevant area of intervention of PSD2, but it is less likely that it will alter the structure of the payments market significantly. On the role of TPPs see also Zachariadis, M. and Ozcan, P. (2017), *The API Economy and Digital Transformation in Financial Services: The Case of Open Banking*, SWIFT Institute Working Paper No. 2016-001. On customer authentication, see Paglietti, C. (2020), *Questioni in materia di prova di pagamenti non autorizzati*, in Paglietti, C. and Vangelisti, M.I. (eds.), *Innovazioni e regole nei pagamenti digitali: il bilanciamento degli interessi nella PSD2*, RomaTre Press.

liquidity and payment services. However, this also makes difficult to obtain a unified picture of the aggregate position across all different accounts, causing organization and synchronization problems. AISPs provide aggregated online information on one or more payment accounts held with one or more other payment service providers. Since better information helps fostering competition, the PSD2 has made it easier for AISPs to access customers' accounts, along similar lines as those defined for PISPs. Indeed, the only difference is that AISPs are not allowed to initiate a payment operation, but they can only gather and provide information to those entities that the account holder has authorized. To this purpose, similar common and open standards of communication are to be implemented. Obviously, like PISPs, AISPs must observe specific data protection and security requirements.

Finally, the PSD2 also allows financial intermediaries to issue card-based payment instruments, such as credit-cards and debit-cards, that directly debit a holder's account held with a different financial intermediary. This allows to break the connection between the issuer of the card and the bank where is held the account that the card debits. As with PISPs and AISPs, holders of customers' accounts are mandated to make them easily accessible to CBPIIs, through standardized APIs.[8]

To assess how the entry of these new players will change the payment industry, we need first to understand what the main levers of competition in this market are, which is the topic of the following section.

---

[8] For a thorough legal analysis of PISPs, AISPs and CBPIIs see also: Profeta, P. (2019), *I third party provider, profile soggettivi e oggettivi*, in Maimeiri, M. and Mancini, M. (eds.), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*, Banca d'Italia, Quaderni di ricerca giuridica 87, settembre 2019; Antonucci, A. (2018), *Mercati dei pagamenti: le dimensioni del digitale*, in *Rivista di diritto bancario* 18, pp. 557-565; Szego, B. (2020), *PDS2 e i nuovi prestatori autorizzati*, in Paglietti, C. and Vangelisti, M.I. (eds.), *Innovazioni e regole nei pagamenti digitali: il bilanciamento degli interessi nella PSD2*, RomaTre Press.

3. Competition in the payment industry

In the past, competition in the market for payments has been low, allowing some players to earn significant extra profits at the expense of their customers. Three main factors favored the emergence of monopoly rents: the possibility to bundle payments with other (banking) services, such as current account services; the presence of large network externalities, due to the fact that the incentive to adopt a new means of payment increases with the number of other individuals adopting it; and the importance of reputation, that hinders the entry of new players in the market. To better understand the role of each one of these three factors in harming competition, it is useful to analyze the steps involved in a typical payment.[9]

Payments are normally the counterpart of a purchase of goods or services, that can take place either physically, for example in a shop, or through the internet. In the case of online purchases of goods, and of some services such as travel tickets and hotel rents, consumption is deferred from the moment of payment.[10] However, an increasing number of services are nowaday accessed and transferred through the internet, such as video and music files, online teaching and consulting services.

From the point of view of its payment, and leaving cash aside, each purchase involves four main steps. First, the customer enters a physical brick and mortar or a virtual shop and chooses the good or service that he wants to buy from the merchant. Second, he transfers an accepted mean of payment from his account to the hands of a financial intermediary providing the payment service (PSP). Third, the PSP transfers the mean of payment to the account of the merchant. Fourth,

[9] On this issue, see also Geerling, M. (2018), *E-commerce: A merchant's perspective on innovative solutions in payments*, in *Journal of Payments Strategy & Systems* 12, pp. 58-67.

[10] For an analysis of the legal implications of payment services, see De Stasio, V. (2016), *Ordine di pagamento non autorizzato e restituzione della moneta*, Giuffré, Milano.

the merchant delivers the good or service acquired, and the purchase is finalized. Although often some steps are even further segmented, as in the case of credit-card payments, we can focus on this simplified framework to understand the determinants of competition in the market, without much loss of generality.

The three factors favoring monopoly rents mentioned above can intervene at different stages of the process. Consider the first, the possibility of bundling payments with other services. An obvious case is when the PSP coincides with the financial intermediary of the customer or of the merchant, which allows to reduce the number of intermediaries involved in the process and, in turn, the cost of the transaction. Financial intermediaries able to offer both payments and deposit services can thus benefit from the economies of scope of providing both activities. This increases the optimal size of operation, making it more difficult for new players specialized only in payment services to enter the market. Eventually, a merchant could even be in the position to agree with his bank to force customers to use a specific PSP, making it impossible for him to choose an alternative. In fact, this is happening increasingly often in the case of some e-commerce websites.

The second factor favoring the emergence of monopoly rents in the payment industry is the presence of network externalities. As already argued above, reducing the number of intermediaries that take part in the payment process is likely to reduce the costs. In principle, if all customers and all merchants held their accounts with the same financial intermediary, that would be the only PSP that is needed, because all payments would involve just the record of a transfer from the account of the customer to that of the merchant. While this is an unlikely outcome in practice, since it would imply the existence of a single monopolistic bank, it remains true that financial intermediaries with a larger number of clients are more likely to be able to settle payments within their own accounts, and therefore to lower costs. This is a clear case of the existence of strong network economies, which favor market concentration.

The third factor, reputation, relates to a key characteristic required of any payment process: that it is secure, i.e. that the transfer is certain. A customer transferring a given amount of money to a PSP wants to be sure that it will then be transferred to the account of the merchant, so that he delivers the good or service that the customer has acquired, and the purchase is finalized. Although PSPs are subject to regulations and supervision, in principle their position allows them to divert the money received, eventually robbing the customer. As a less fraudulent alternative, PSPs can economize on their investment in information technologies, reducing their standards of security and therefore increasing the probability that the information on the payment is lost. This makes it harder for an unknown financial intermediary to enter the market for the provision of payment services, because customers are unlikely to trust transferring their money in his hands. PSPs need therefore to gain a reputation for being reliable, something that typically requires time and is often associated with size. Again, this limits entry in the market for payments, favoring concentration and monopoly rents. In fact, customers in many countries seem to have a preference for making their payments through traditional banks, possibly because of their better reputation.

4. PSD2 and competition in the payment sector

Judging from the picture described above, PSD2 will foster competition by favoring the entry of new players in the second and third phase of the payment process: the transfer from the account of the buyer to the PSP and that from the PSP to the account of the merchant. By allowing PISPs to directly initiate a payment process and AISPs to rationalize the management of payments from different accounts, PSD2 aims at favoring the entry of players which may be able to innovate the existing services, exploit better technological know-how, accept lower profit margins – offering

better and cheaper services overall. Reassuringly, PSD2 also requires PSP to be subject to a set of regulations aimed at guaranteeing the security of the services that they offer. Will this work?

A payment is very similar to what economists define as a commodity good, because its characteristics make it easily exchangeable across different suppliers. A key feature of competition in markets for commodity goods is that it is only based on prices. If a purchase can be paid with two different payment cards, and one has a lower cost, a rational economic agent would never use the other card. However, this analysis is correct only if we focus exclusively on the payment, i.e., on the activity of transferring a mean of payment from the account of the buyer to that of the seller. In fact, without taking into account riskiness, payments can be extremely different depending on at least two additional characteristics: how easy it is to make them and how quickly the transfer is made. Overall, entrants can gain market shares if they are able to provide a payment experience that improves on the existing ones along one of four dimensions: because it is cheaper, it is easier, it is quicker, or it is less risky. On which one of these characteristics are entrants more likely to have a competitive hedge?

Two main reasons suggest that price competition is likely to be relevant only on the merchant side of the market. First, the structure of interchange fees is such that the costs of a payment is mainly born by merchants. In fact, in most countries, the cost of a good or service cannot be different depending on the mean of payment that it used to pay for its purchase.[11] Second, the cost of the single payments is

[11] There are many reasons why this is the case. From an economic perspective, the literature on two-sided markets has shown that charging merchants is in many cases the profit-maximizing strategy of competing payment service providers (see the ample literature that refers to the seminal paper by Rochet, J-C. and Tirole, J. (2003), *Platform Competition in Two-Sided Markets*, in *Journal of the European Economic Association* 1, pp. 990–1029. From a legal perspective, see Doria, M. (2011), *Commento all'art. 3, d.lgs. n. 11/2010*, in Mancini, M., Rispoli Farina, M., Santoro, V., Sciarrone Alibrandi, A. and Troiano, O. (eds.), *La nuova disciplina dei servizi di pagamento*, Giappichelli, Torino, and Broggiato (2019), *Profili competitivi e consumeristici del divieto di surcharge*, in Maimeiri, M. and Mancini, M. (eds.), *Le*

already relatively low, and it is unlikely that possible reductions allowed by better technologies will be so large to motivate consumers to switch from one PSP to another: it is therefore the merchant that may have an incentive to push for the adoption of cheaper means of payment.

A price-based competitive advantage is therefore more likely to emerge if a PSP has a better ability to process payments. A crucial example is that of closed loop systems, i.e., "systems set up and operated by a single payment service provider", in which consumers and merchants hold an account with the same financial intermediary. Examples of these systems are US-based PayPal, Chinese Alipay, and Italian Satispay. Within a closed loop system, a payment entails only two opposite records: in the accounts of the consumer and in that of the merchant. Consequently, it does not require the transfer of information across different accounting systems, as in the case of a transfer of funds from the account of one bank to another. The competitive advantage of closed loop systems with respect to more traditional processes involving banks or credit card systems is thus the result of their ability to process payments at lower costs. Clearly, the incentive for merchants to hold an account with a closed loop system is increasing in the number of consumers using it as a mean of payment, and symmetrically the incentive for consumers is increasing in the number of merchants that offer it as a mean of payment. This is a major source of network economies: the larger the number of users, the lower the costs.[12]

Remarkably, PSD2 excludes closed loop systems from the obligation to allow access to AISPs, PISPs and CBIIPs through standardized APIs, thus giving them a significant regulatory advantage with respect to other PSPs. I will come back to this issue below.

---

nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale, Banca d'Italia, Quaderni di ricerca giuridica 87, settembre 2019.

[12] In addition, closed loop systems may be in the position of earning an interest rate margin, if they are allowed to invest the funds of their customers at higher rates than those that they pay on the accounts held with them.

As already argued above, risk can be an important factor influencing the choice of the PSP. However, in all developed countries, payment institutions are heavily regulated and supervised along all crucial dimensions: technological, organizational and financial.[13] For example, financial intermediaries issuing Electronic money, as well as PISPs and CBPIIs, cannot accept deposits from users and can only use funds received from users for payment services. Moreover, they must respect initial capital requirements. Since regulation creates a level playing field, it is unlikely that riskiness may become a crucial competitive factor in the supply of payments services within the same country. Riskiness can indeed be a crucial characteristic in the case of cross-border payments, but it is likely that once a given threshold of safety is guaranteed, competition will be on other features.

Aside from prices and riskiness, competition will most likely be based on how easy and quick it is to make a payment, limiting the number of steps required to make it. Let's consider in-shop purchases first. With cash payments, the transfer is typically very swift, with the only nuisance of requiring to hold the right amount of change. With electronic payments, readiness has increased significantly in recent years. In the past, all electronic payments required to insert a plastic card into a device that connected remotely, typically via a phone call, and printed a receipt that had to be signed in order to authenticate the transaction. The process could easily last around one minute. Some improvements have initially come with the substitution of the signature authentication with that based on the personal identification number (PIN). More recently, contactless payments of small-amount transactions, with no requirement of authentication, have made the payment process as swift as that of cash payments, and without the problem of having the right

[13] European Banking Authority (EBA) has been required to define the technical standards of secure communication between Third Party Providers (TPPs) and the financial intermediaries where the accounts are held.

amount of change. Contactless payments using a smartphone with a biological identification device can be as swift as that with a card, but with the advantage of being potentially less risky.

Only the adoption of cheaper and better technologies seems capable of offering a better payment experience in the case of in-shop purchases. By using a smartphone it is possible to transmit a large amount of data, thus allowing to perform two crucial steps of an in-shop payment: authentication and transfer. The smartphone industry is very concentrated: four corporations (Samsung, Huawei, Apple and Oppo) are responsible of half of total world production of devices, and only two operating systems are used in practice: Android and iOS. But these corporations do not offer payment services autonomously, preferring to partner with different financial intermediaries. Since producers of smartphones do not have incentives to make an exclusive partnership with just one provider of financial services, technological innovation stemming from hardware improvements is unlikely to be a key competitive factor for payment service providers, and the new players introduced by PSD2 are unlikely to have a major role.

A different case is that of software improvements. Although only two operating systems are used in the market, competition could stem from the ability of payment service providers to interface with these systems, making their apps swifter and more user-friendly. By allowing PISPs and CBPIIs to enter this sector, PSD2 may alter competition dynamics also in the case in-shop payments.[14]

In the case of online purchases, payments can at times be rather cumbersome: customers may be required to type their cards' codes: the PIN, and the one time password (OTP) that they receive through different means of communication – typically small text

[14] A different issue, that is also part of PSD2 but is not analyzed in this chapter, is the reimbursement of fraudulent transactions. Better authentication systems, leading to a lower number of frauds and higher reimbursement rates, could also be source of competitive advantage.

messages (SMS) or, less commonly, e-mails. Completing these tasks may require a few minutes and can be rather complicated, with the risk that a purchase is not completed or the payment is made to the wrong counterpart. It is therefore no surprise that new services are being provided, allowing to register in smartphones or computers a set of information that make electronic payments easier and quicker.

In the case of internet-based transactions, purchases and payments are much more connected, and there is no reasonable alternative to electronic payments.[15] Internet-based merchants have a stronger incentive to offer a better payment experience, because the cost of switching to a different merchant is much smaller on the web than across traditional brick and mortar shops. Internet based merchants are thus among those that could benefit the most from becoming a PISP, because in this way they could link the purchase with the payment, offering the best possible customer experience. Bundling purchases and payments can therefore be more effective than in the case of brick and mortar shops. Clearly, since setting up a PISP involves relevant fixed and sunk costs, big-techs like Amazon, which can dilute these costs across their large consumer base, may be more likely to exploit the possibilities offered by PSP2.

However, the previous discussion on cost advantages of closed-loop systems suggests that setting up a PISP may not be the best solution for e-commerce platforms. In fact, PayPal itself was initially created to make swifter payments on E-bay, the website specialized in consumer-to-consumer and business-to-consumer sales, and Alipay is linked to Alibaba, the largest e-commerce platform in China. PayPal and Alipay are closely linked to the e-commerce platform and are thus able to offer an easy and swift payment experience. But

[15] Some goods can still be paid in cash to the delivery man, and services such as hotel rents booked in advance on the internet can be paid when checking-out with different means of payment from those used to make the reservation. However, the incidence of these transactions is small and decreasing.

they are also closed loop systems, thus benefitting from lower costs and the potential to earn positive interest margins. Big-techs like Amazon may therefore prefer to set up their own closed loop system instead of creating a PISP, as Alibaba has already done with Alipay.

As mentioned above, PSD2 favors closed loop systems, arguing that "it would not be appropriate to grant third parties access to those closed proprietary payment systems". Allegedly, this choice is made "in order to stimulate the competition that can be provided by such closed payment systems to established mainstream payment systems". But will the entry of these players foster competition in the payment industry? Since big-techs enjoy massive network economies of scale, it may indeed be the case that their closed loop systems allow swifter and easier payments at lower costs. At the same time, the optimal minimum scale of operations may be so large to allow for very few players in the market, thus hindering competition. As it is always the case with natural monopolies, finding an equilibrium between competition and efficiency is not easy. But it may be worth to consider granting third parties access to closed loop systems, since they already benefit from large network economies.

One additional argument stands in favor of not granting privileges to big-techs operating in the payment industry, and possibly limiting their expansion: the value of the information that they can collect. So far, our discussion has focused mainly on making a payment, i.e., on PISP and possibly on CBIIP. But with the explicit authorization of customers, these new types of intermediaries, as well as AISPs, can collect, store and elaborate information on each single payment for a potentially enormous number of consumers all over the world. If payments are managed by an in-house PISP or closed-loop system of an e-commerce platform, each payment can easily be linked with the purchase that caused it. Clearly, such information has an enormous value, for example for marketing and credit-scoring purposes. In Europe, the General Data Protection Regulation (GDPR) seems to be the only boundary to potential abuses in this field. Additional efforts in this direction seems warranted.

5. Conclusions

With few exceptions, I am generally in favor of any policy aiming at improving competition, because it increases aggregate economic welfare. In most cases, helping entrants in a market improves competition, and therefore I see it as a positive step. But markets in which bundling and network economies cause strong economies of scale is one of the exceptions to the general rule. Entry of large and powerful players can in this case reduce competition, with a negative impact on aggregate welfare.

The direction taken by the PSD2 is correct: favoring the entry of new players, reducing the benefits of holding proprietary information, dismantling the bundling of different services related to payments will improve competition and increase welfare. But attention must be paid to two possible risks.

The first risk is that big-techs exploit economies of scale, related to network effects and the possibility of bundling different services, to gain large market shares and hinder competition. Allowing third parties to access closed loop systems may be an important step to avoid this outcome.

The second risk is related to data collection and management. As emphasized by Gammaldi and Iacomini (2019),[16] "[t]he Directive indeed introduces the concept according to which data are available to the customer who 'generated' them". This allows all players in the payment industry – including big-techs, if they are willing to enter this market – to collect information on payments linked with those on purchases, in addition to what they already collect, for example through social media. The use of information credit risk evaluation and price discrimination can have a disruptive effect on

[16] Gammaldi, D. and Iacomini, C. (2019), *Mutamenti del mercato dopo la PSD2*, in Maimeiri, M. and Mancini, M. (eds.), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*, Banca d'Italia, Quaderni di ricerca giuridica 87, settembre 2019.

the financial market. Moreover, individuals may misperceive the immediate benefits that they obtain by releasing their data, and the often uncertain future costs related to their use on the part of specialized operators. In this context, "the explicit consent (freely expressed by users) may no longer be sufficient to guarantee respect for privacy", as argued by Menzella (2019).[17]

The risks caused by data mismanagement should be forcefully contrasted, within and outside the financial industry. For this reason, each specific piece of legislation should coordinate with the provisions of the GDPR.[18] Moreover, to guarantee all players using individual data and derived elaborations a level playing field, it should be considered to allow third parties to access the information collected by big-techs, according to the same philosophy which led the regulator to permit AISPs to access information collected by financial intermediaries, when users gave their consent. Of course, any such policy should be mirrored by initiatives aiming at making citizens aware of the value of their personal information – with a specific focus on financially-related information – for example offering "privacy education" in addition to "financial education".

[17] Menzella, R. (2019), *Il ruolo dei big data e il mobile payment*, in Maimeiri, M. and Mancini, M. (eds.), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*, Banca d'Italia, Quaderni di ricerca giuridica 87, settembre 2019.

[18] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). On this issue, see Rabitti, M. (2020), PSD2 e riparto di competenze tra autorità amministrative indipendenti, in Paglietti, C. and Vangelisti, M.I. (eds.), *Innovazioni e regole nei pagamenti digitali: il bilanciamento degli interessi nella PSD2*, RomaTre Press.

Gustavo Olivieri
(LUISS University - Rome)

PSD2, MIF AND ANTITRUST ENFORCEMENT IN THE NEW MARKETS FOR ONLINE PAYMENT SERVICES

1. Foreword: the Multilateral Interchange Fee (MIF) between competition and regulation

My speech will be mainly focused on competition enforcement, *i.e.* the application of antitrust law in the new markets for payment services, and only incidentally on Multilateral Interchange Fee Regulation.

The reason for this choice lies not only in the need to stay within the time limits assigned to me, but also in a more general approach of systematic nature which recommends to keep the functions carried out by competition and market regulation separate.

In this regard, it is customary to state that regulation defines *ex ante* the playing field on which companies operate, while the protection offered by antitrust law intervenes only *ex post* to sanction any possible conduct that may restrict competition, such as agreements or abuses of dominant position.

Equally widespread is the observation that an *ex ante* regulation of a given activity becomes necessary in the presence of market failures, *i.e.* the situations where the mechanisms of decentralized choice of companies do not ensure the desired effects in terms of reduction of costs, quantity and quality of goods offered in the market ([1]).

[1] On the relationship between competition and regulation see, *ex multis*, AA.VVV, *Regolazione e concorrenza*, edited by G. Tesauro and M. D'Alberti, Bologna, 2000, and therein S. CASSESE, *Regolazione e concorrenza*, 11 et seq.; M. MONTI, *Concorrenza e regolazione nell'Unione Europea*, 75 et seq.

This is what occurred in relation to the costs of certain payment services and explains the origin of numerous interventions of the EU legislator on Multilateral Interchange Fee (MIF), culminating in Reg. no. 2015/751 of April 29, 2015 relating to interchange fees for card-based payment transactions. One of the recitals of that Regulation states that:

> *"Interchange fees are usually applied between the card-acquiring payment service providers and the card-issuing payment service providers belonging to a certain payment card scheme.*
> *Interchange fees constitute a major component of the fees charged to merchants by acquiring payment service providers for every card-based payment transaction. Merchants in turn incorporate those card costs, like all their other costs, in the general prices of goods and services.*
> *Competition between payment card schemes to convince payment service providers to issue their cards leads to* ***higher*** *rather than lower interchange fees , in contrast with the usual price-disciplining effect of competition in a market economy.*
> *In addition to a consistent application of the competition rules to interchange fees, regulating such fees would improve the functioning of the internal market and contribute to reducing transaction costs for consumers"* (recital 10 of Reg. no. 2015/751).

The thesis according to which the sub-optimal development of card payment instruments represents a market failure that should be remedied by means of an *ex ante* regulation of the prices applied by intermediaries, rather than occasional *ex post* fines levied by the Antitrust Authorities, seems to be shared both at national and EU level ([2]).

After all, the wide recourse to the instrument of closure of proceedings with commitments by the companies within the investigations launched for violation of the prohibition of agreements restricting competition

[2] V. MELI, *Gli interventi dell'Autorità nei sistemi di pagamento*, in Atti del Convegno di Trento.

found in recent years ([3]) already denotes a trend of the Competition Authorities to surreptitiously regulate the phenomenon.

The provisions contained in articles 34-*bis* et seq. of Legislative Decree no. 218/2017 implementing the PSD2 Directive, which set regulatory limits on the amount of interchange fees applicable to payment transactions carried out with debit cards for consumer use, also fall within this perspective.

Therefore, I will not address these regulatory profile, although I am aware that they inevitably affect the market for debit card payment services as well as competition among the companies that provide those services.

As it has recently been observed, the evolution in progress leads one to foresee that "in the context of the payment instruments subject to the Regulation of April 2015 – there will hardly still be a propulsive role of antitrust in relation to the MIF and the NDR [Non Discriminatory Rule, ed.], while it is foreseeable that there will be further developments in regulation" (MELI, op. cit., p. 16).

However, not wishing to evade the task I have been assigned, I will limit myself to a few quick general remarks, which can be summarized as follows:

- the 2015 Reg. placed a lower limit on the MIF than that indicated by AGCM in the several proceedings closed with commitments, thus effectively making the Authority's intervention unnecessary;
- in cases of MIF not covered by the Regulation (*e.g.*, that relating to ATM service on cash withdrawals) the limit imposed by antitrust decisions remains in place;
- in the case of bill payments (the so-called *Bill Payment* case no. I773D), which are also subject to the cap indicated by the EU Regulation, the Authority considers that the cap indicated by the regulator is too high and the Bancomat consortium committed to lower the relevant MIF;

[3] See cases *Visa MIF* of the EU Commission 2010 and 2014 and AGCM, *Bill Payments* of 2014.

- with regards to relations between AGCM and Bank of Italy, the unwritten rule followed up to now is that the Antitrust Authority deals with the MIF regarding "non-capped" services, while the Supervisory Authority deals with "capped" services, unless there are specific reasons for imposing a MIF lower than the regulatory cap through the antitrust instrument.

2. PSD2 and *Unbundling* of payment services

After this brief introduction, I would now like to examine the provisions implementing the PSD2 Directive which, in my opinion, are more relevant from an antitrust law standpoint, starting with those which intervene on the definition of the relevant market and of the players authorized to operate in it.

From this point of view, there is no doubt that the new discipline of payment services in the internal market is destined to significantly expand both the range of products offered to customers and the number of competing companies, thus modifying the competitive ecosystem in which banks have operated until now to the benefit of end users.

In this context, it has been authoritatively observed that "the push for greater competition in the sector comes from the fact that, with the new directive, current accounts are also opened to non-banks: that is, the client will be able to authorize a third party to access his account and give instructions without the bank being able to intervene" ([4]).

As a result, the consumer will have the opportunity "to benefit from new financial services provided by TPPs [Third Party Providers]" using the infrastructure provided by banks.

The impact resulting from this proper *Unbundling* of banking and financial services connected or linkable to a payment account in terms of lowering barriers to entry is substantial.

[4] PITRUZZELLA, *Fintech e i nuovi scenari competitivi nel settore bancario, finanziario e assicurativo*, ABI, 10 May 2018, p. 4.

In particular, as pointed out in a study published by CONSOB ([5]) "the regulations that guarantee open and shared access to payment accounts for the use and provision of new online payment services [*i.e.* Internet based] have in themselves the potential to determine the evolution of operating configurations and new business models" that go beyond that specific area, to include banking, financial, social security and insurance services.

From a subjective point of view, the PSD2 Directive aims at further increasing competition in the payment services sector by introducing and regulating a new type of operator, the **Third Party Providers**, in addition to those already present in the market for payment services and differing from both the "account rooting" PSPs and the Electronic money institutions, as they do not intervene in the management of payment accounts nor in the circulation of funds available to the holder.

These new players – pursuant to art. 2, para. 1, Legislative Decree no. 218/2017 – may therefore alternatively be framed in the notion of:

a) providers of payment order services ("payment institutions");
b) entities exclusively providing account information services.

2.1. The structure of the new markets for payment services

Differently from what used to happen in the past with the correspondence current account, to which the bank linked a bundling of services that made the possible acquisition of customers by competitors extremely difficult ([6]), the new provisions provide for the possibility of unbundling payment services and accessory services linked to payment accounts, thus

---

[5] *Financial Data Aggregation e Account Information Services. Questioni regolamentari e profili di business*, edited by Bianchi, Mezzacapo, Musile, Tanzi, Troiano, March 2018, p. 13.

[6] On this point, see the AGCM's fact-finding survey no. IC32 of January 2007 regarding prices for retail banking services.

modifying the structure and perimeter of the relevant markets from an antitrust viewpoint.

In particular, it seems useful to distinguish between downstream markets for the provision of payment and non-payment services, which are separate (also in terms of authorized players to operate in them) from the upstream market where companies offering payment account servicing (provision and administration) operate, thus representing a necessary facility for operating in downstream markets.

The payment account is therefore placed at the center, or rather at the top, of a new system of value creation consisting of a wide range of innovative value-added activities, services and products (credit, investment, insurance and pension) whose supply presupposes the possibility of accessing the information contained in the payment account.

2.2. The Right to Access to payer's information

It is therefore easy to understand how, in this changed perspective, a key role will be played by the rule that provides the holder of the payment account with a real right to access the information contained therein and therefore to the computer systems of the account rooting PSPs, with the right to make use for this purpose also of third party companies operating on behalf of the holder.

The obligation for the intermediaries with whom the payment account is set up to ensure access to the information contained therein under fair and non-discriminatory conditions is also of considerable importance. It is clear that the conditions of access and use of this particular facility are likely to determine foreclosure or partitioning effects on different downstream markets such as, for example, those for the provision of payment orders and account information.

The practice of margin squeeze in vertically integrated markets is well known to the Antitrust Authorities, which also in this case have to ensure that the conditions applied by the intermediary with

whom the payment account is established, or by those who offer this access service on behalf of the banks, are not such as to squeeze the margins of competitors in downstream markets ([7]).

Similarly, the reasons for any refusal or delay in accessing payment account information will need to be carefully considered to ensure that they do not conceal a form of "constructive boycott" against payment service providers in downstream markets.

On the other hand, in the absence of an express request in this regard from the holder of the payment account, it would seem more difficult to outline the existence of an obligation on the bank to grant access to the information contained in the payment accounts by the provider of the new services along the lines of what is envisaged by the so-called *Essential Facility Doctrine* for companies with vertically integrated essential infrastructures ([8]).

While it is indeed true that access to payment accounts is a prerequisite for being able to provide services in downstream markets, it seems hard to argue that payment service providers of account rooting are in a dominant position with respect to the availability of information about their customers and as such are subject to a general obligation to ensure access to these essential inputs on fair and non-discriminatory conditions ([9]).

---

[7] For some examples of such practice in the markets for communication services, see AGCM's decision no. 24339, *Condotte abusive di Telecom Italia*, in Bull. no. 20/2013; CJ EU, C-280/08, *Deutsche Telekom*.

[8] See, e.g., AGCM's decision no. 26907 – *Società Iniziative Editoriali*, in Bull. no. 51/2017; EU Comm. 21-12-1993, *Sea Containers/Stena Link*, in OJ 1994, L15, and more recently AGCM's investigation A-529 launched by the Authority against Google.

[9] Moreover, such a view would be in line with what AGCM stated in the case no. A-357 (decision no. 17131 of 3.8.2007) with reference to fixed-mobile termination services offered by the companies operating in the retail market for telephony (Tim, Vodafone, Wind), where the Authority acknowledged the existence of a dominant position of each operator with reference to the phone calls addressed to its own subscribers.

Without further stressing this point, it is however clear that the legislator's intention was to prevent those operating in the upstream market for the management of payment accounts from engaging in practices aimed at preventing or delaying the entry of new competitors into the downstream services indicated above.

This package of rules includes not only the previously mentioned obligation to allow such parties access to the information and operating systems that handle payment orders – at the customer's request – on fair and non-discriminatory conditions.

With the same vision, it is also worth mentioning the regulation of limits on access to payment accounts by payment service providers.

Pursuant to art. 5-*quater,* para. 8, of the Decree at hand, an account rooting service provider may deny access to a payment account to an information service provider or to a payment order service provider [only] "for justifiable and demonstrable reasons related to fraudulent or unauthorized access to the payment account by such entities".

Particularly interesting, again with a view to avoiding unequal treatment, appears the rule that requires the provider of rooting account payment service to ensure "equal treatment of orders transmitted through a payment order service provider compared to those transmitted directly by the payer, except for objective reasons referring, in particular, to the applicable time, priority or charges" (art. 5-*ter*, para. 3(c), Legislative Decree no. 218/2017).

Equality of treatment to be understood, in this case, as the obligation not to discriminate against payment orders transmitted via another provider not only from a technical but also an economic point of view. It would therefore seem precluded for banks the possibility to set a different fee for the same service depending on how the payment order is executed.

On the other hand, the aforementioned provision leaves open the question, particularly relevant from a competitive standpoint, of whether – and, if so, to what extent – banks can charge service companies that request access to their customers' current accounts.

The analogy with the provisions for other liberalized network services (in particular, the unbundling of the local loop in the telecommunications market, or the energy and transport sectors) should lead one to believe that also in the case of the new "liberalized" payment services the network owners (*i.e.* the banks) have the right to be remunerated for allowing competitors access to their infrastructures (*i.e.* the rooting accounts and the information contained therein) ([10]).

In any event, a different solution, based on the tendency of the service to be free of charge, should be the subject of a specific (and temporary) asymmetrical regulatory measure aimed at favoring the entry of new players in the market while avoiding, at the same time, free-riding phenomena.

3. Cooperation between competitors and possible concerns from an antitrust viewpoint

Nonetheless, it cannot be ruled out that the implementation of PSD2 may also give rise to behaviors that are relevant from an antitrust standpoint, such as restrictive agreements or abuse of dominant position.

It is foreseeable that the opening up of a series of services to new operators may lead incumbents to obstacle new comers. These conducts do fall within the competence of the Antitrust Authority, even if at the moment we don't know what kind of infringements we will be dealing with. However, it has been recalled that "in the past, the Authority has already received complaints from operators

[10] On this point, see VV. AA., *Il nuovo diritto dell'energia tra regolazione e concorrenza*, edited by Eugenio Bruti Liberati-Filippo Donati, Turin, Giappichelli, 2007. On the effects of asymmetric tariffs in the telephone services markets, see HURKENS-LOPEZ, *The Welfare Effects Of Mobile Termination Rate Regulation In Asymmetric Oligopolies: The Case Of Spain*, 2011, who argue that tariff asymmetry, although positive for smaller companies, generally leads to less collective welfare.

who felt they were being hindered by banks in their entry into the payments market" ([11]).

Therefore, "any obstacles by the banks to the entry of new operators... could, in abstract terms, amount to antitrust violations in the case of conduct agreed between banks that could fall under the prohibition of restrictive agreements" ([12]).

The explicit collusion aimed at excluding competitors is a serious infringement of competition rules and could hardly find adequate justification in a benefit for consumers, under the conditions set out in paragraph 3 of Article 101 TFEU.

Differently, the compliance with Antitrust law of agreements between competitors aimed at facilitating online access to the accounts and information of payment service clients by new entrants through the creation of cooperative joint ventures, , must be examined in the light of the traditional criteria used for this purpose by European Union case law.

4. Digital Platforms and online payment services

It is more difficult to imagine, in the new competitive scenario that will be created following the implementation of PSD2, the adoption by single operators of unilateral conduct capable of producing exclusionary effects to the detriment of competitors. As well known, such conduct is relevant under antitrust law only if carried out by companies in a dominant position; an assumption that seems difficult to meet in Italy, given that no bank – except for specific local situations or particular product markets – holds such a high degree of market power.

However, it cannot be ruled out *a priori* the possibility of exclusionary abuses of dominant position in the new markets for (electronic) payment services.

---

[11] MELI, *PSD2 – Opportunità e sfide per la concorrenza*, p. 9.

[12] MELI, op. ult. cit., p. 10.

From this point of view it could be relevant to consider, on the one hand, "the particular position that each bank holds in relation to access to the accounts of its clients, similar in some respects to the already ascertained monopoly position held by telephone operators with reference to the termination of calls", could play an important role ([13]).

On the other hand, it should be noted that some of the new entrants in the online payment services markets are represented by companies that already enjoy significant competitive advantages and benefit from wide dominant positions in their respective markets of origin. Reference is made, obviously, to the so-called **Over the Top** companies (Google, Facebook, Apple, Amazon) which "could leverage the market power they hold elsewhere to enter the payment services", for example, by charging prices or other economic conditions that cannot be replicated by equally efficient competitors.

The project for the creation of a new crypto-currency called Libra, recently announced by Facebook, seems to confirm the thesis of those who, also in Brussels, pay attention to the moves of the web giants and to the market power they are able to exercise thanks to the collection and use of data on a large scale for commercial purposes ([14]).

FinTech and the new online payment services represent contiguous markets which – as it has been pointed out by many – well expose themselves to a massive exploitation through AI (Artificial Intelligence) systems of the information contained in client payment accounts in order to offer a vast range of banking, financial, insurance and social security services ([15]).

---

[13] MELI, op. cit., p. 10.

[14] Some news on the operating scheme of Libra can be found in R. DE BONIS-M.I. VANGELISTI, *Moneta. Dai buoi di Omero ai Bitcoin,* Bologna, 2019.

[15] On this point, see FALCE-FINOCCHIARO, *La Digital Revolution nel settore finanziario*, in *Algoritmi: se li conosci li eviti*, edited by Nuzzo and Olivieri, AGE/1/2019; PITRUZZELLA, *Fintech e i nuovi scenari competitivi*, loc. cit., p. 6.

It is therefore not surprising that giants such as Google, Apple, Facebook and Amazon are destined to play a leading role in the markets for payment services opened up by PSD2, not only as drivers of significant technological innovations, but also as challenging competitors to the banking system. ([16]).

[16] On this point, see R. DE BONIS-M.I. VANGELISTI, *Moneta*, cit., 167 et seq., where also interesting considerations on the strategies of the network giants (Google, Amazon, Facebook) with reference to new payment services can be found.

Robert Freitag[1]
(Maître en droit)

PSD2 AND OTHER EU-DIRECTIVES IN THE BANKING AND FINANCIAL SECTOR
The Case of the Directives on Electronic money and on the Distance Marketing of Financial Services

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market etc.[2] (hereinafter "PSD2) interacts in various manners with other instruments of EU secondary legislation. Out of the plethora of possible subjects, this contribution will focus on two exceptionally relevant issues, i.e. on the neighboring 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 on Electronic money etc.[3] (hereinafter "EMD2") and on the Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services etc.[4] This selection seems especially fruitful as it allows for a combination of issues of a primarily supervisory nature (EMD2) with mainly private law aspects of payment services (Directive 2002/65/EC) in the context of digitalization of payment services.

---

[1] The author is professor at the Faculty of Law of the University of Erlangen-Nuremberg and judge at the Higher Regional Court of Nuremberg.

[2] OJ 2015 L 337/35.

[3] OJ 2009 L 267/7.

[4] OJ 2002 L 271/16.

A. Interactions between PSD2 and EMD2

The second E-money directive EMD2 constitutes an incremental update and modernization of its legal predecessor, the former first E-money directive EMD1 which dated from 2000.[5] Before going into details, it is worth looking at some statistics to better assess the practical importance of Electronic money (hereinafter: E-money) in the internal market: All national registers confounded, EBA currently counts 372 E-money institutions registered in the EU.[6] The amount of E-money issued has continuously risen from the unregulated beginnings prior to the entry into force and applicability of EMD1[7] until today.[8] Whereas this process has initially been rather slow, the amount of deposits in E-money has all but exploded in the past decade. The reasons for this surge (which is not subject to profound research by the author) cannot be based on the appearance of EMD2 as this directive is applied since April 30th 2011 only. However, the seemingly impressive success of E-money has to put into perspective. A closer look at the relevant figures shows that the market share of E-money indeed has risen, but not as spectacularly as was to be expected. At least as far as the mere number[9] of payments is concerned, E-money does not represent more than about four per cent. of all non-cash-payments within

[5] 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, OJ 2000 L 275/39.

[6] See https://euclid.eba.europa.eu/register/pir/search (consulted 07.02.2020).

[7] EMD1 was to be implemented by Member Stats no later than 27th April 2002, see art. 10 para. (1) EMD1.

[8] See ECB statistics 2018, http://sdw.ecb.europa.eu/reports.do?node=1000003509 (consulted on 07.02.2020).

[9] See ECB payment statistics 2019, http://sdw.ecb.europa.eu/servlet/desis?-node=1000004051, p. 14 et seq. (consulted on 07.02.2020). As to the amounts transferred see ECB payment statistics 2019, http://sdw.ecb.europa.eu/servlet/desis?node=1000004051, p. 29 (consulted on 07.02.2020).

the EU. Also, the number of payment service providers offering payment services to non-MFI significantly exceeds the number of Electronic money institutions by (approximately) the factor 20.[10] The use of E-money as well as the importance of services related thereto obviously evolve rather slowly. It is noteworthy, however, that GooglePay has obtained an E-money-licence in Lithuania recently which is valid for the entire Single Market under the single licence-principle of EMD2.[11]

1. Scope of Application of EMD2 (Definition of E-money)

As regards the legal concept of E-money, EMD1 and EMD2 aim at providing legal certainty on the subject by defining the term. The relevant definition, which is contained in art. 2 no. 2 EMD2[12] reads as follows:

> "<Electronic money> means an 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 and which is accepted by a natural or legal person other than the Electronic money issuer".

Most of the criteria named in this definition do not exclusively apply to E-money but also to traditional scriptural money booked in a bank account because also scriptural money is (i) stored electronically,

---

[10] Statista counted 7321 "institutions offering payment services to non-MFIs in the European Union (EU) in 2018 (https://www.statista.com/statistics/443018/payment-service-provision-european-union/, consulted on 07.02.2020), among which figure 5170 MFIs (see https://www.ecb.europa.eu/stats/ecb_statistics/escb/html/table.en.html?id=JDF_MFI_MFI_LIST, consulted on 07.02.2020).

[11] S. art. 3 par. (1) EMD2 in conjunction with art. 28 PSD2.

[12] Art. 1 para. (3) lit. (b) EMD1 had an almost identical wording. The only material difference between the definitions of E-money by EMD1 and EMD2 relates to the definition of possible "points of sale" which accept E-money as means of payment: Under EMD1, E-money needed to be accepted by enterprises, whereas under EMD2 the acceptance by any natural or legal person suffices.

(ii) represents a claim against the relevant payment institution and (iii) may be and usually is used for payment transactions and (iv) is accepted by natural or legal persons other than the issuer. As regards the relevant point(s) of differentiation, it would be tempting to argue that E-money is issued by the relevant Electronic money institution as defined by art. 2 no. 1 EMD2, i.e by a private enterprise, whereas scriptural money is issued by a central bank, i.e. by a governmental agency. This approach, although formally in compliance with the aforementioned definition, does not suffice to distinguish both phenomena. Scriptural money and E-money share the commonality that they constitute mere claims for payment of the customer against a financial institution. Furthermore, E-money is not conceived as a distinct currency but is closely linked to the official currency of the currency area in which the E-money-account is held. This can be derived from (i) art. 11 para. (1) EMD2, pursuant to which E-money must be issued "at par value on the receipts of funds", as well as from (ii) art. 11 para. (2) EMD2, which states that E-money is redeemable upon the request of the E-money holder at par value at any time. The aforementioned rules indirectly imply that E-money must be denominated in the local currency, thus linking it to the local currency regulations in an indirect manner. However, the aforementioned similarities between scriptural and Electronic money already hint at their pivotal difference. Scriptural money is more closely linked to the local currency and central bank than E-money. The holder of scriptural money "stored" on a payment account may claim from the bank the disbursement of the positive balance of the bank account in legal tender whereas the customer of an E-money institution may only claim a credit transfer to a bank account, i.e. may demand the exchange of E-money against a claim for scriptural money. Furthermore, E-money institutions may not accept deposits from the public under art. 6 para. (2) EMD2 and consequently any positive balance on an E-money account may not bear any (positive) interest as per art. 12 EMD2.[13] In sum, E-money is a

[13] Obviously, this rule has lost most of its impact in times of negative interest rates for deposits on ordinary payment and/or deposit accounts.

special version of scriptural money held with a specifically regulated non-bank. E-money may either be stored on a payment card or booked on an account held with an E-money institution. Payments in E-money are subject to the same rules as those made in scriptural money because PSD2 applies to both phenomena: Pursuant to its art. 1 para. (1) and art. 2 para. (1), PSD2 lays down the rules applicable to "payment sevices", which art. 4 no. (3) PSD2 defines as the services mentioned in Annex 1 to PSD2. According to no. 3 of Annex 1 of PSD2 (as well as to art. 2 para. (2) PSD2), the term "payment services" encompasses the administration of "payment transactions" as per art. 4 no. (5), i.e. an act of placing, transferring or withdrawing "funds". Pursuant to art. 4 no. (25), "funds" are defined as "banknotes and coins, scriptural money or Electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC".[14] Economically speaking, E-money-institutions are therefore financial institutions that issue payment units denominated in local currency usable for electronic payments and redeemable at any time against scriptural money. The pivotal economic advantage of E-money is that payments with E-money can be executed inside the ecosystem of the relevant E-money-institution and are thus cheaper and faster than ordinary credit transfers from one bank to another.

The higher court of Berlin recently ruled that bitcoins do not constitute E-money under EMD2.[15] The court correctly based its judgement on three pivotal arguments: First, there is no centralized issuer of bitcoins, second bitcoin-investors do not have a claim against anyone for the redemption of their bitcoins against scriptural money, let alone against legal tender, third bitcoin-investors may not demand that bitcoins are accepted as means of payment. It seems that also Facebook's project for "Libra" will not be construed in such manner as

[14] The obviously outdated and thus erroneus link of PSD2 to EMD1 has to as if referring EMD2 since the date of applicability of EMD2.

[15] Kammergericht Berlin, judgement of 25.09.2018, case (4) 161 Ss 28/18 (35/18), Neue Juristische Wochenschau 2018, 3734.

to fall within the scope of application of EMD2: Although the Libra foundation in Geneva will serve as central issuer ("central bank"), Libra-holders will have no claim against the Libra foundation for redemption of libra nor may they claim acceptance of Libra by sellers. In other words, bitcoins and libra are designed to constitute real private currencies entering into competition with official currencies. They differ from one another in that only Libra will be subject to a centralized (private) authority which will control the amount of circulating Libra as well as the composition of the currency basket underlying Libra. In contrast, bitcoins are completely decentralized, i.e. there is no instance which has any discretionary power over the currency, the fate of which is exclusively determined by the bitcoin-algorithm. Another question not to be answered in this context is whether the issuance of private currencies is compatible with the exclusive competence of the EU in monetary matters under art. 3 (1) lit c) TFEU.[16]

2. Interactions between EMD2 and PSD2

EMD2 and PSD2 interact in various manners and it is thus advisable to distinguish between the private law aspects of the issue and regulatory matters.

As regards private law rules applicable to payment transactions, it has been shown above (under 1.) that PSD2 also governs payment transactions in E-money, i.e. the respective rights and obligations of E-money-users and E-money-institutions relating to payments in E-money are therefore identical to those of ordinary users of payment services and their PSP.

In contrast, the issuance and redemption of E-money are exclusively governed by EMD2. With regard to the framework

[16] See ECB, Occasional Paper Series (May 2019), Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf (consulted on 10.02.2020).

agreements which lay down the respective rights and obligations of the financial institution and its customers, it would seem that the conclusion of and subsequent changes to framework agreements do not constitute "payment transactions" as per art. 4 (4) PSD2 and therefore do not apply to accounts for E-money. However, the aim of framework agreements is to specify the rights and obligations of the parties with regard to payment transactions and the holding of payment accounts. It is therefore consequent that art. 50 PSD2 states that Title III, Chapter 3 of PSD2 "applies to payment transactions covered by a framework contract" and thus also to E-money.

As regards regulatory issues, the amount of initial and own funds to be held by E-money institutions significantly exceeds that mandatory for ordinary PSP under PSD2.[17] The stricter rules for E-money institutions are based on the valid consideration that an E-money institution must at all times be able to meet the claims of its customers for the redemption of the entire amount of E-money issued; in contrast, ordinary PSP only pose a risk to their customers with regard to the amounts currently handled by them for the purpose of transfers.[18] As regards the scope of eligible activities, the rules applicable to ordinary PSP under PSD2 and to E-money-institutions are quite similar[19] and the rules relating to EU-passporting[20] are identical, those applicable to the remaining aspects of prudential supervision are very close and art. 3 para. (1) EMD2 therefore incorporates the majority of applicable provisions of PSD2 into EMD2.

---

[17] Under art. 7 PSD2, the initial capital of an ordinary payment service provider is to be at least 20.000 EUR, 50.000 EUR or 125.000 EUR (depending on the services offered), whereas under art. 4 EMD2 the initial capital of an E-money-institutions must be at least 350.000 EUR. The calculation of own funds pursuant to art. 8, art. 9 PSD2, art. 5 EMD2 adds additional differences to the already distinct regime of capital requirements.

[18] S. recital (11) of EMD2.

[19] S. art. 6 EMD2, art. 18 PSD2.

[20] See art. 28 PSD2, art. 3 para. (1) EMD2.

3. Conclusion

The aforementioned differences between ordinary payment service providers and E-money-institutions do not justify the existence od a "stand alone-directive" for E-money institutions. The commonalities of both types of providers of payment services outweigh the minor differences and it is thus highly advisable to incorporate the rules on E-money into a "wholesale" directive on electronic payments which covers "ordinary" payment services providers as well as those issuing E-money. Such a consolidation would help to reduce the complexity of applicable legislation without necessitating to ignore the specifics of E-money.

B. Interactions between PSD2 and Directive 2002/65/EC

Directive 2002/65/EC on the distance marketing of financial services is the remaining dinosaur of the members of the first wave of EU consumer protection laws. In contrast to the former Directives 97/7/EC on the distance marketing of goods and "ordinary services"[21] and Directive 85/577/EEC on consumer contacts concluded outside of business premises,[22] it has been left untouched by the EU's effort to modernize, simplify and unify consumer legislation through the Consumer Rights Directive 2011/83:[23] Art. 3 para. (3) lit. (d) of the Consumer Rights Directive explicitly exempts contacts for financial services (as defined by art. 2 para. (12) of that directive) from the scope of its

[21] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, OJ L 144/19.

[22] Directive of 20 December 1985 to protect the consumer in respect of contracts negotiated away from business premises (85/577/EEC), OJ L 372/31.

[23] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights etc., OJ L 304/64.

application because the legislator did not want to interfere with existing specialized legislation in the field of financial services.[24] This exemption, in conjunction with the abolition of Directive 85/577/EEC by art. 31 of the Consumer Rights Directive, has the unforeseen consequence that consumers who have entered into contracts for financial services outside of business premises no longer have a right of withdrawal under EU law.[25] As regards framework contracts concluded between consumers on the one hand and payment services providers under PSD2 or E-money institutions under EMD2 on the other hand by means of telecommunication, solely Directive 2002/65/EC applies. This has two major consequences:

First, Directive 2002/65/EC follows a two-step-approach regarding the pre-contractual information duties of the business – a concept which is unique to this directive and unknown especially under the Consumer Rights Directive: On the first level, a financial service provider offering distance contracts must provide general information as to himself and his products in a manner "suitable to the distribution channel", i.e. on his website. This general and preliminary information shall enable the consumer to decide on an informed basis whether to pursue the possible conclusion of a contract with the relevant business. Art. 39 and art. 110 PSD2 modify these rules with a view to the specifics of payment services. The second level of information duties as regulated by art. 5 of Directive 2002/65 relates to the phase immediately prior to the conclusion of a distance contract: The financial services provider – must in due time before a specific contract for financial services is to be agreed upon – inform the

[24] See recital (32) Consumer Rights Directive.

[25] By its famous decision dated 13 December 2001 in the case C-481/99 „Georg und Helga Heininger/Bayerische Hypo- und Vereinsbank AG", the CJEU had correctly stated that Directive 85/577/EEC was applicable also to consumer contracts for financial services (including mortgage credits).

consumer not only (once again?) on all aspects already covered by art. 3 of the directive, but also on the terms and conditions of the specifically envisaged contract the consumer is about to conclude. This second set of information has to be given on paper or on another durable medium accessible to the consumer, thus enabling the latter to store and reproduce the information in the future. The CJEU has provided guidance on this subject by its "BAWAG"-judgment from 2017.[26]

The most powerful means of consumer protection is enshrined in art. 6 of Directive 2002/65 on the consumer's unconditional right of withdrawal, which parallels art. 9 of the Consumer Rights Directive. The consumer may withdraw from the contract within 14 days after the later of (i) the time of conclusion of the contract and (ii) the time the necessary pre-contractual information under art. 5 of the directive has been correctly and completely given. In case the payment service provider has not complied with his information duties, the consumer may withdraw from the contract for a potentially indeterminate period. This unacceptable consequence has led national legislation and jurisprudence to subject the right of withdrawal to the rules on forfeiture (*Verwirkung*).[27] But purely national remedies do not suffice to generally immunize framework agreements concluded on the internet or by phone against the consequences of late withdrawals based on incorrect or missing pre-contractual information: Such immunization is necessary as a late withdrawal would deprive all authorizations for individual payment transactions of their contractual foundation which clearly is imcompatible with the idea that authorized and executed payments are "untouchable"

[26] CJEU 25.1.2017, case C-375/15 „BAWAG PSK", for details see *Freitag*, ZIP 2018, p. 1805, 1807 et seq.

[27] See with regard to the former directive 85/577/EEC the judgement CJEU 10.04.2008, case C-412/06 "Hamilton" no. 32, et seq.

under art. 80 PSD2. One must therefore argue that PSD2 as lex posterior and lex specialis prevails over the earlier and more general Directive 2002/65.

Finally, it is worth mentioning that Art. 6 para. (2) lit. (a) of Directive 2002/65 excludes the right of withdrawal „if the service includes financial services whose price depends on fluctuations in the financial market outside the suppliers control, which may occur during the withdrawal period, such as services related to foreign exchange". This exemption applies to payment transactions under art. 43 et seq. PSD2 to be executed in a foreign currency involving a floating exchange rate. In contrast, it seems doubtful whether one may deprive the consumer of his right to withdraw from a framework agreement only because a single future authorization for an individual payment may possibly relate to a payment in a foreign currency.

This leads to the conclusion that Directive 2002/65/EC on the distance marketing of financial services is in imminent need of an overhaul as it no longer reflects current standards of EU-consumer legislation. The Commission has therefore for just cause launched a public consultation on potential changes to the directive in 2019. In my opinion, it would be advisable to integrate the contents of Directive 2002/65/EC into the general regime of the Consumer Rights Directive. This would lead to more legal certainty and simplification as the rules applicable to distance contracts would be united in one single legal act. A unification of the rules applicable to distance contracts for "ordinary" services and for financial services would also allow for a streamlining of the applicable material regimes, namely with regard to the lapse of the right of withdrawal after a maximum period of 12 months and 14 days after the conclusion of the contract as well as in case the service provider has started to execute the contract upon the consumer's express wish. Furthermore, the pre-contractual information duties under art. 3 of Directive 2002/65/EC, which does not serve a useful purpose, could be eliminated in the process.

C. Final Remarks

This brief survey of PSD2 and its closest neighbors EMD2 and Directive 2002/65 on the distance marketing of financial services leads to the conclusion that the law of payment services requires a more homogenous legal regime with regard to the private law aspects of payment services as well as to the prudential supervision of payment services providers (including E-money institutions). A first important step to be taken by the European legislator into this direction would consist of the integration of EMD2 into PSD2 and of Directive 2002/65 into the Consumer Rights Directive. This would create a more level playing field for all payment service providers in a digitalized market for payments and would reduce unnecessary complexity of European consumer protection law. Whether the European legislator will pursue this path is doubtful, but not to be excluded. And it remains to be noted that a simplification of applicable legislation can never exclude the occurrence of complex legal problems which require solutions tailored to the specific needs of the subject of electronic payment services.

II PARTE / *SECOND PART*

GLI EFFETTI DELL'ATTUAZIONE DELLA PSD2 SULLA TUTELA DEI CLIENTI / *THE IMPACT OF THE TRANSPOSITION OF PSD2 ON CUSTOMER PROTECTION*

Simone Mezzacapo[1]
(Università degli Studi di Perugia)

PSD2, ONLINE AND MOBILE PAYMENTS: WHAT TRANSPARENCY FOR THE FUTURE OF PAYMENTS?

Summary: 1. The EU payment services regulatory framework. – 2. The transparency on the scope of PSD2. – 3. The transparency on pricing and information. – 4. The transparency on the terms of execution of payment transactions. – 5. The transparency and security of the Internet and mobile payments: Strong Customer Authentication (SCA), dynamic-linking and communication standards. – 6. The PSD2 rule-based approach and the need for an enforcement moratorium *on SCA requirements.*

1. The EU payment services regulatory framework.

The Directive (EU) 2015/2366 (PSD2)[2] is part of an EU "legislative package" on retail payment services, including the Regulation (EU) 2015/751 on card-based payment transactions[3]. The PSD2 specifically revises and updates the EU legal framework formerly established on the matter by the Directive 2007/64/EC (PSD1)[4].

---

[1] Professore Associato di Diritto dell'Economia - Università degli Studi di Perugia.

[2] Directive (EU) 2015/2366 of The European parliament and of the Council of 25.11.2015 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.

[3] Regulation (EU) 2015/751 of the European Parliament and of the Council of 29.4.2015 on interchange fees for card-based payment transactions.

[4] Directive 2007/64/EC of the European Parliament and of the Council of 13.11.2007 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.

The PSD2 aims not only at achieving "further integration of an internal market in payment services"[5] but also, or better primarily, to keep up with what represents an actual "paradigm shift" triggered by the prominent "technologically enabled financial innovation" (or FinTech solutions)[6] lately experienced also within the EU retail payments market, specifically a "rapid growth in the number of electronic and mobile payments and the emergence of new types of payment services in the market place, which challenges"[7], inter alia, the appropriateness and consistency of the EU regulatory framework on payment services based on the PSD1[8].

[5] See recital 3 of the PSD2.

[6] See Bank for International Settlements and Financial Stability Board, FinTech credit. Market structure, business models and financial stability implications – Report by a Working Group established by the Committee on the Global Financial System (CGFS) and the Financial Stability Board (FSB), Bank for International Settlements and Financial Stability Board, 22.5.2017, p. 2, Valerio Lemma, *FinTech Regulation. Exploring New Challenges of the Capital Markets Union*, Palgrave Macmillan, 2020, p. 13..

[7] See recital 3 of PSD2.

[8] In particular, as specified, the "review of the Union legal framework on payment services and, in particular, the analysis of the impact of Directive 2007/64/EC and the consultation on the Commission Green Paper of 11 January 2012, entitled, 'Towards an integrated European market for card, internet and mobile payments', have shown that developments have given rise to significant challenges from a regulatory perspective. Significant areas of the payments market, in particular card, internet and mobile payments, remain fragmented along national borders. Many innovative payment products or services do not fall, entirely or in large part, within the scope of Directive 2007/64/EC. Furthermore, the scope of Directive 2007/64/EC and, in particular, the elements excluded from its scope, such as certain payment-related activities, has proved in some cases to be too ambiguous, too general or simply outdated, taking into account market developments. This has resulted in legal uncertainty, potential security risks in the payment chain and a lack of consumer protection in certain areas. It has proven difficult for payment service providers to launch innovative, safe and easy-to-use digital payment services and to provide consumers and retailers with effective, convenient and secure payment methods in the Union. In that context, there is a large positive potential which needs to be more consistently explored", recital 4 of PSD2.

In this context the new rules and principles of PSD2 are intended essentially to enable users of retail payment services in the EU to benefit from the new opportunities offered by such innovations, whilst setting higher transparency and security standards for electronic payments, to ultimately promote "the development of a sound environment for e-commerce"[9], as well as more competition in the EU internal market[10].

Nevertheless, it is to be noted that the PSD2 does not provide for a comprehensive regulation of "payments" (*i.e.* the settlement of monetary obligations) in the EU internal market[11], but it rather regulates "only" the services for the "handling" of funds, or namely the operations of placing, transferring or withdrawing "funds", irrespective of any underlying obligations between the payer and the payee[12].

It implies, among other things, that the PSD2 does not come out in a *legal vacuum*, it coexists instead with numerous other EU and national laws and regulations also applicable to "payments" and of pivotal importance for the actual execution of online and mobile payments in the EU internal market, namely *inter alia*: *a)* EC Regulation "Rome I" on the law applicable to contractual obligations[13] and the national provisions on monetary obligations

---

[9] See recital 95 of PSD2.

[10] See Fabio Porta, Obiettivi e strumenti della PSD2, in AA.VV., *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, cripto valute e rivoluzione digitale, edited by* F. Maimeri and M. Mancini, Banca d'Italia, *Quaderni di Ricerca Giuridica della Consulenza Legale*, n. 87, settembre 2019 p. 21.

[11] See also: Vincenzo De Stasio, *Operazioni di pagamento non autorizzate e restituzione*, Educatt, Milano, 2013.

[12] See Antonella Sciarrone Alibrandi, L'adempimento dell'obbligazione pecuniaria tra diritto vivente e portata regolatoria indiretta della Payment services directive 2007/64/CE, in AA.VV., *Il nuovo quadro normativo comunitario dei servizi di pagamento. Prime riflessioni*, edited by Marco Mancini e Marino Perassi, BANCA D'ITALIA, *Quaderni di Ricerca Giuridica della Consulenza Legale*, n. 63, Dicembre 2008, p. 61.

[13] Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I).

(in Italy mainly set forth in the Civil Code); *b)* Directive 2011/83/EU[14] on consumer rights and Directive 2002/65/EC on the distance marketing of consumer financial services[15] (as implemented in Italy in the *Consumer Code*[16] which also establishes provisions on the application of fees and charges for payment services); *c)* mentioned Regulation (EU) 2015/751 capping interchange fees and establishing a set of *business rules* on card-based payments[17]; *d)* Directive 2014/92/EU (*Payment Account Directive* or PAD)[18] on the transparency and comparability of fees connected with payment accounts, the rights to switch payment accounts and of access to payment accounts with basic features; *e)* Regulation (EU) n. 260/2012[19] on technical and business requirements for credit transfers and direct debits in euro, including, for example,

[14] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council.

[15] 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

[16] Decreto Legislativo 6 settembre 2005, n. 206, Codice del consumo, a norma dell'art. 7 della legge 29 luglio 2003, n. 229.

[17] See Fabrizio Maimeri, *La disciplina dei costi e delle commissioni interbancarie nella PSD2*, in Banca d'Italia, *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, cripto valute e rivoluzione digitale*, edited by Fabrizio Maimeri and Marco Mancini, *Quaderni di Ricerca Giuridica della Consulenza Legale*, n. 87, settembre 2019, p. 83. Simone Mezzacapo, La nuova disciplina UE dei limiti alle interchange fees e delle business rules in materia di "pagamenti basati su carte", tra regolamentazione strutturale del mercato interno e promozione della concorrenza, in *Diritto della banca e del mercato finanziario*, n. 3/2017, p. 455.

[18] Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features.

[19] 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.

the ban to so-called "*IBAN discrimination*")[20]; *f)* GDPR 2016[21] as regards, *inter alia*, the online processing of payment data and information in the context of the new "open banking" scenario; *g)* the EU and national antitrust legislations; *h)* the EU and national regulations of telecommunication services (*e.g.* in Italy the *Electronic Communications Code*[22]); *i)* last but not least, the EU and national provisions on the taking-up and pursuit of the business of banks, financial intermediaries and e-money institutions (in Italy primarily laid down in the *Consolidated Banking Code*[23]).

In such complex, multi-layered and not always consistent legal framework, the PSD2 has the merit to add some more clarity and transparency as to the regulatory treatment to be applied to innovative solutions for the provision "on-line" or "on-the-go" of traditional (cashless) payment services, as well as certain new types of payment services, primarily by better defining the scope of application of EU rules and principles on the provision within the EU "internal market" of retail payment services.

For example, compared to PSD1, the PSD2 brings into the (positive) scope of application of EU retail payment services regulation

---

[20] A practice that has been recently subject of enforcement actions by the Italian Competition Authority pursuant to the combined application of Article 9 of Regulation (EU) n. 260/2012 and the provisions of the Italian Consumer Code on unfair commercial practices, see Resolutions n. 27642 of 10 April 2019 (*PV2 – Vodafone – Discriminazione Iban esteri*), n. 27643 of 10 April 2019 (*PV3 – Wind – Discriminazione Iban esteri*), n. 27644 of 10 April 2019 (*PV4 – Telecom – Discriminazione Iban esteri*), n. 27645 of 10 April 2019 (*PV5 – Fastweb – Discriminazione Iban esteri*).

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

[22] Decreto Legislativo 1 agosto 2003, n. 259, Codice delle comunicazioni elettroniche.

[23] Decreto legislativo 1° settembre 1993, n. 385, Testo unico delle leggi in materia bancaria e creditizia.

two new types of services which, instead, were so far considered as "mere" IT services. Specifically, under the PSD2 the *business activities* that make up the regulatory category of *payment service* now include also those defined as *Payment Initiation Services* (PIS) and *Account Information Services* (AIS) (points 7 and 8 of Annex I to PSD2). The *Payment Service Providers* (PSPs) specialized in the provision of such newly regulated *payments services* make up the category of *Third Party Payment Services Providers* (TPPs)[24], which according to PSD2 taxonomy is made of *Payment Initiation Services Providers* (PISPs)[25] and *Account Information Service Providers* (AISPs)[26].

One of the most distinguishing features of PIS and AIS is that their performance is dependent on the possibility for the relevant TPPs to enjoy open access to *payment accounts* maintained and/or serviced by (one or more) other PSPs that within the PSD2 are referred to as *Account Servicing Payment Service Providers* (ASPSPs)[27].

On the contrary, it is important to highlight that the legal definition of *payment account* has not been substantially changed by the PSD2 compared to the PSD1 (see Article 4, point 12, of PSD2 and Article 14, point 14, of PSD1) and is also mutually consistent with that of the almost coeval PAD (see Article 2, point 3)[28].

---

[24] See Domenico Gammaldi – Costanza Iacomini, *Mutamenti del mercato dopo la PSD2*, in Banca d'Italia, *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, cripto valute e rivoluzione digitale*, edited by Fabrizio Maimeri and Marco Mancini, *Quaderni di Ricerca Giuridica della Consulenza Legale*, n. 87, settembre 2019, p. 123.

[25] See article 4, points 15 and 18 of PSD2.

[26] See article 4, points 16 and 19 of PSD2.

[27] See article 4, point 17 of PSD2. For the relating competition issues see: Simone Mezzacapo, *Competition policy issues in EU retail payment business: the new PSD 2 regulatory principle of open on-line access to information from "payment accounts" and associated "payment transactions"*, in *European Competition Law Review*, Vol. 39, Issue 12 [(2018) 39 E.C.L.R., Issue 12], p. 534.

[28] With regard the more simpler payment service referred to as "money remittance", which is typically a payment service not based on a payment account but rather based on cash provided by a payer to a PSP, which remits the

The consistency on this point between the PSD2 and the PAD is of key importance, because the legal definition of *payment account* in the EU *aquis* is intended to be neutral toward different legal, contractual and technical arrangements, and so it entails the risk of being over-inclusive and giving rise to legal uncertainties and disputes[29]. Should it be the case the PAD constitutes the pivotal reference to be used to settle any interpretative issues on the matter, as lately also established by the Court of Justice of the European Union (CJEU) in a judgment of 2018 (Case C191/17) relating to the interpretation of the notion of *payment account* as in Article 4(14) of PSD1[30].

---

corresponding amount, for example via a communication network, to a payee or to PSP acting on behalf of the payee and its difference with other "informal" payments systems, see Moliterni Francesco, *I sistemi di pagamento informali fra rimesse di denaro e contratto di rete*, Giuffrè, Milano, 2019, p. 98; Vittorio Santoro, *I servizi di pagamento, in Ianus*, n. 6/2012, p. 12.

[29] See: Simone Mezzacapo, *La nuova disciplina nazionale dei "conti di pagamento" alla luce dell'armonizzazione attuata con la Payment Accounts Directive*, in *Banca Borsa e Titoli di Credito*, n. 6/2017, p. 787.

[30] In its judgment – relating to a request for a preliminary ruling made in a national proceedings concerning the lawfulness of the standard terms and conditions of the contracts offered by an Austrian bank – the Court specifically noted that it "*is also set out in recital 14 of the Payment Accounts Directive that the definitions contained in that directive had to be aligned as far as possible with those contained in other Union legislative acts, and in particular with those contained in the Payment Services Directive*" and, as a result, an account from which "*payment transactions cannot be made directly, but for which use of an intermediary account is necessary, cannot therefore be regarded as being a 'payment account' within the meaning of the Payment Accounts Directive and, consequently, within the meaning of the Payment Services Directive*" (points 16 and 32 respectively of the judgment of the Court (Fifth Chamber) of 4 October 2018, Bundeskammer für Arbeiter und Angestellte v ING-DiBa Direktbank Austria Niederlassung der ING-DiBa AG, Request for a preliminary ruling from the Oberster Gerichtshof, Case C-191/17). See also: Simone Mezzacapo, *La vexata quaestio della qualificazione della fattispecie giuridica di "conto di pagamento" ai sensi e per gli effetti della diritto UE dei servizi di pagamento nel "mercato interno"*, in *Diritto della Banca e del Mercato Finanziario*, n. 4/2019, p. 695..

2. The transparency on the scope of PSD2

As regards the positive scope of application of EU retail payment services law, while the PSD1 typically applied to intra-EU payment transactions, on the contrary, the PSD2 caters for the extension, except for some provisions, of the scope of its *transparency* and *information* requirements (*i.e.* Title III of PSD2), and *rights and obligations* in relation to the provision and use of payment services (*i.e.* Title IV of PSD2), also to certain types of *international payments* which are typically processed or executed *on-line* o via *mobile devices* within the context of *global e-commerce trades* (i.e. to and from third countries).

Specifically, the PSD2 now explicitly provides that its Titles III and IV (except for certain provisions) also apply to any payment transaction in "non-EU currencies" (*i.e.* a currency that is not the currency of an EU Member State) where both the payer's PSP and the payee's PSP are located within the Union or if the sole PSP involved in the payment transaction is located within the Union (Article 2(3) PSD2). It is also now clearly provided that Titles III and IV of PSD2 (except for certain provisions) also apply to any payment transactions irrespective of the currency used (namely "in all currencies") where only one of the PSP is located within the Union (Article 2(4) PSD2)[31].

Nevertheless, so as to avoid extraterritorial effects of EU law, the application of such PSD2 rules is anyhow explicitly limited "to those parts of the payments transaction which are carried out in the

[31] As noted, such "extension of the scope has implications primarily for the banks and other payment service providers that are located in the EU. In practice, this means that these financial services providers shall provide information and transparency on the costs and conditions of these international payments, at least in respect of their part of the transaction. They can also be held liable for their part of the payment transaction if something goes wrong that is attributable to them. Moreover, the extension in scope will also have as an effect that the same rules will apply to payments that are made in a currency that is not denominated in Euro or another Member State's currency", European Commission, Payment Services Directive: frequently asked questions, Memo, Brussels, 12 January 2018.

Union" (Article 2(3) and (4) PSD2)[32]. A concept further reinforced by the provision that in general the PSD2 only "applies to payment services provided within the Union" (Article 2(1) PSD2).

This means that PSD2 provisions on *transparency* and *information* requirements and certain *rights and obligations* could now apply also to payment transactions in any currency where one of the PSPs involved (*e.g.* the PSP of the payee/merchant or the PSP of the payer) is located outside the European Economic Area (EEA), yet for the parts of the transactions executed or processed in the EU[33].

Furthermore, also so-called *one-leg out* or *one-leg in* transactions in any currency (*e.g.* those in favor of non-EU PSPs when at least one of the other PSPs involved is located within the EU), previously not covered by the PSD1, could now (partially) fall within the scope of most of PSD2 provisions on *transparency* and *information* requirements and certain *rights and obligations*, including, although only "on a best-effort basis", also those on *Strong Customer Authentication* (SCA)[34].

---

[32] As noted, such "extension of the scope has implications primarily for the banks and other payment service providers that are located in the EU. In practice, this means that these financial services providers shall provide information and transparency on the costs and conditions of these international payments, at least in respect of their part of the transaction. They can also be held liable for their part of the payment transaction if something goes wrong that is attributable to them. Moreover, the extension in scope will also have as an effect that the same rules will apply to payments that are made in a currency that is not denominated in Euro or another Member State's currency", European Commission, Payment Services Directive: frequently asked questions, Memo, Brussels, 12 January 2018.

[33] As specified in the provisions of PSD2 "*on transparency and information requirements for payment service providers and on rights and obligations in relation to the provision and use of payment services should also apply, where appropriate, to transactions where one of the payment service providers is located outside the European Economic Area (EEA) in order to avoid divergent approaches across Member States to the detriment of consumers. Where appropriate, those provisions should be extended to transactions in all official currencies between payment service providers that are located within the EEA*" (recital 8 of PSD2).

[34] Indeed, as clarified by the EBA and "explained in the final report on the draft RTS published in February 2017, the EBA's view, after discussing it with the European Commission, is that SCA applies to all payment transactions initiated by a payer, including to card payment transactions that are initiated through the payee within the EEA and apply only on a best-effort basis for cross-border transactions with one leg out

Besides that, the PSD2 also provides for a much more harmonized and detailed regulation of security, transparency, interoperability, and open communication requirements to be complied with in the use, initiation and/or execution of "electronic payments", as well as of associated responsibility and liability regime. The PSD2 framework on the matter is specifically based on the considerations that "the security risks relating to electronic payments have increased"[35], while on the other hand "security of electronic payments is fundamental for ensuring […] the development of a sound environment for e-commerce"[36] and a "solid growth of internet payments and mobile payments should be accompanied by a generalized enhancement of security measures[37]. In this respect another distinguishing aspect of PSD2 is that its provisions on the matter are complemented by a detailed set of Regulatory Technical Standards on "authentication and communication" to be developed by the EBA, in close cooperation with the ECB, and formally adopted by delegated regulations of the European Commission (Article 98 of PSD2).

As to the scope of application of the EU *acquis* on retail payment services, the PSD2 also specifies more transparently and uniformly the perimeter of its *negative scope*, namely by setting forth a list of more detailed possible *exclusions* from its regulatory framework.

Regarding the new EU regulation of *on-line* and *mobile*[38] payments, the most relevant exclusions from the PSD2 are those

---

of the EEA. In such a case, the liability regime stated by Article 74(2) PSD2 applies", Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC, EBA-Op-2018-04, 13 June 2018, point 32.

[35] See recital 7 of PSD2.

[36] See recital 95 of PSD2.

[37] See recital 95 of PSD2.

[38] As correctly pointed out the expression "mobile payments" actually refers to a composite phenomenon which includes typically : 1) *Mobile Remote Payment*; 2) *Mobile Commerce*; 3) *Mobile Money Transfer*; 4) *Mobile Proximity Payment*, see Raffaella Menzella, *Il ruolo dei big data e il mobile payment*, in AA.VV., *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, cripto valute e rivoluzione digitale*, edited by F. Maimeri and M. Mancini, Banca d'Italia, *Quaderni di Ricerca Giuridica della Consulenza Legale*, n. 87, settembre 2019, p. 153.

relating to: *i) commercial agents*, which is of particular interest for the functioning of e-commerce platforms; *ii) limited use* or *limited networks*; *iii)* the so-called *telecom exemption*.

In particular, based on the consideration (and concern) that the existing exclusion from the scope of PSD1 of payment transactions through a *commercial agent* had been applied "*very differently across the Member States*", so allowing a different regulatory treatment also of *e-commerce* platforms[39], the PSD2 provides that an exemption for commercial agents "involved" in payment transactions could apply where an agent is authorised "to *negotiate or conclude the sale or purchase of goods or services on behalf of only the payer or only the payee*" (Article 3 (b) PSD2), even if the agent temporarily comes "*in possession of client funds*". On the contrary, if a commercial agent acts "*on behalf of both the payer and the payee (such as certain e-commerce platform)*" the exclusion from the scope of PSD2 is conditional on the fact that the agent does *"not, at any time enter into possession or control of client funds*"[40].

Regarding the other exclusion, already provided also under the PSD1, for "services based on specific payment instruments that can be used only" within "limited networks" or to acquire a "very limited range of goods or services", in order to limit the excessively heterogeneous and too indulgent approaches adopted in the national applications of such exclusion under the PSD1, the PSD2 now specifies more precisely the requisites of eligible *limited networks*[41]

---

[39] Indeed as specified, "*Certain Member States* [... allowed the use of the exclusion from the scope of PSD1 of payment transactions through a commercial agent even …] *by e-commerce platforms that act as an intermediary on behalf of both individual buyers and sellers without a real margin to negotiate or conclude the sale or purchase of goods or services. Such application of the exclusion goes beyond the intended scope set out in that Directive and has the potential to increase risks for consumers, as those providers remain outside the protection of the legal framework. Differing application practices also distort competition in the payment market*", recital 11 of PSD2.

[40] Recital 11 of PSD2.

[41] For example, it has been clarified that payment instruments "covered by the limited network exclusion could include store cards, fuel cards, membership cards,

and *specific-purpose instruments*[42], and also details other conditions to be met for the legitimate reliance on such exclusion (Article 3(k) of PSD2)[43]. For example, it has been introduced an obligation for PSPs to notify, in case, their "*competent authorities of the activities that they provide in the framework of a limited network* […] *if the value of payment transactions exceeds a certain threshold*"[44], the objective being

public transport cards, parking ticketing, meal vouchers or vouchers for specific services, which are sometimes subject to a specific tax or labour legal framework designed to promote the use of such instruments to meet the objectives laid down in social legislation", recital 14 of PSD2.

[42] As a general principle, if a *specific-purpose instrument* covered by the *limited network exclusion* develops into a *general-purpose instrument* such exclusion ceases to be applicable, in the same vein "instruments which can be used for purchases in stores of listed merchants should not be excluded from the scope of [… the PSD2 …] as such instruments are typically designed for a network of service providers which is continuously growing", recital 14 of PSD2.

[43] In particular, as noted, feedback "from the market shows that the payment activities covered by the limited network exclusion often comprise significant payment volumes and values and offer to consumers hundreds or thousands of different products and services. That does not fit the purpose of the limited network exclusion as provided for in Directive 2007/64/EC and implies greater risks and no legal protection for payment service users, in particular consumers, and clear disadvantages for regulated market actors. To help limit those risks, it should not be possible to use the same instrument to make payment transactions to acquire goods and services within more than one limited network or to acquire an unlimited range of goods and services. A payment instrument should be considered to be used within such a limited network if it can be used only in the following circumstances: first, for the purchase of goods and services in a specific retailer or specific retail chain, where the entities involved are directly linked by a commercial agreement which for example provides for the use of a single payment brand and that payment brand is used at the points of sale and appears, where feasible, on the payment instrument that can be used there; second, for the purchase of a very limited range of goods or services, such as where the scope of use is effectively limited to a closed number of functionally connected goods or services regardless of the geographical location of the point of sale; or third, where the payment instrument is regulated by a national or regional public authority for specific social or tax purposes to acquire specific goods or services", recital 13 of PSD2.

[44] Recital 20 of PSD2.

to allow the authorities to "*assess whether the activities so notified can be considered to be activities provided in the framework of a limited network*"[45] (Article 37 of PSD2). On the other hand, such exclusion has been extended to certain *domestic payment instruments* (*i.e.* valid only in a single Member State) having "*specific social or tax purposes*" (Article 3(k)(iii) of PSD2).

Finally, it is worth noting that the PSD2 gives continuity to the PSD1 regulatory approach according to which – under certain conditions – payment transactions executed by means of telecom or information technology devices could be also excluded from the scope of EU payment services regulation, this due to the persistent absence of "evidence that such payment transactions, trusted by consumers as convenient for low-threshold payments, have developed into a general payment intermediation service"[46]. The application of this exclusion has allowed for example the development in the EU of "so-called operator billing or direct to phone-bill purchases" of digital contents and services[47].

Nevertheless, to the benefit of transparency and legal certainty, the PSD2 clarifies and tightens the conditions to be met for the application of this so-called "*telecom exemption*", because "it has been implemented differently across Member States, leading to a lack of legal certainty for operators and consumers and occasionally allowing payment intermediation services to claim eligibility for an unlimited exclusion from the scope of"[48] the PSD1.

---

[45] Recital 20 of PSD2.

[46] Recital 14 of PSD2.

[47] For example those "*services include entertainment, such as chat, downloads such as video, music and games, information such as on weather, news, sports updates, stocks and directory enquiries, TV and radio participation such as voting, competition entry, and provision of live feedback. Feedback from the market shows no evidence that such payment transactions, trusted by consumers as convenient for low-threshold payments, have developed into a general payment intermediation service*", recital 15 of PSD2.

[48] Recital 15 of PSD2.

As a result, Article 3(l) of PSD2 confirms, on one hand, that the "*telecom exemption*" still ideally covers low-value payments for "purchase of digital content and voice-based services, regardless of the device used for the purchase or consumption of the digital content and charged to the related bill", and on the other it introduces a clear reference to payment transactions "performed from or via an electronic device and charged to the related bill within the framework of a charitable activity or for the purchase of tickets"[49]. Moreover, Article 3(l) the PSD2 provides that in any case the *telecom exemption* "should apply only where the value of payment transactions is below a specified threshold in order to limit it clearly to payments with a low risk profile"[50]. In particular, value of any single payment transaction covered by this exemption should "not exceed EUR 50 and: (i) the cumulative value of payment transactions for an individual subscriber does not exceed EUR 300 per month, or (ii) where a subscriber pre-funds its account with the provider of the electronic communications network or service, the cumulative value of payment transactions does not exceed EUR 300 per month".

[49] The rationale of the exclusion of donations to charities is to "ease the burden on entities that collect charitable donations", yet Member States are "free to limit the exclusion to donations collected in favour of registered charitable organizations". Instead, the exclusion relating to payments for the purchase of electronic tickets has been introduced "to take into account the development in payments where, in particular, customers can order, pay for, obtain and validate electronic tickets from any location and at any time using mobile phones or other devices. Electronic tickets allow and facilitate the delivery of services that consumers could otherwise purchase in paper ticket form and include transport, entertainment, car parking, and entry to venues, but exclude physical goods. They thus reduce the production and distribution costs connected with traditional paper-based ticketing channels and increase customer convenience by providing new and simple ways to purchase tickets", Recital 16 of PSD2.

[50] Recital 16 of PSD2.

3. The transparency on pricing and information

The PSD2 provisions on charges applicable to payment services are based on, and further bolster, a policy approach according to which within the internal market any payer and payee should in principle bear only the charges possibly levied directly on them by their respective PSPs, pursuant to the contract terms in place with the same PSPs[51]. In doing so, the PSD2 primarily strengthens and broadens the scope of application of the so-called "SHA" charging option (*i.e.* shared costs) by providing that it applies to all payment transactions "provided within the Union" irrespective of the currency used (Article 62(2) PSD2)[52].

The PSD2 also establishes that, in principle, no additional charges should be imposed for the provision of certain information to consumers or, in other words, it provides for a right for consumers to receive mandatory information free of charges, in particular "before being bound by any payment service contract […, and also to …] request prior information as well as the framework contract, on paper, free of charge at any time during the contractual relationship". The objective is to ensure to consumers due transparency and comparability on the services and conditions offered by PSPs and enable them "to verify their contractual rights and obligations, thereby maintaining a high level of consumer protection"[53].

In particular, Article 40 of PSD2 provides that PSPs shall not charge the payment service user (PSU) for providing mandatory

[51] Indeed, it has been considered that "experience has shown that the sharing of charges between a payer and a payee is the most efficient system since it facilitates the straight-through processing of payments", recital 65 of PSD2.

[52] In particular it is therein provided that "Member States shall require that for payment transactions provided within the Union, where both the payer's and the payee's payment service providers are, or the sole payment service provider in the payment transaction is, located therein, the payee pays the charges levied by his payment service provider, and the payer pays the charges levied by his payment service provider".

[53] Recital 59 of PSD2.

information under Title III of PSD2 which establishes the new EU rules on transparency of conditions and information requirements for payment services.

However, to allow for the flexibility necessary to take into consideration different consumer needs, it is provided that instead charges could be applied if "more frequent or additional information, or transmission by means of communication other than those specified in the framework contract" is requested by PSPs' clients (Article 40(2) of PSD2).

Following the different national practices observed in the EU as to the charges applied for the provision of "monthly statements of payment accounts on paper or in another durable medium", the PSD2 leaves to Member States to decide whether to impose that also such statements are always to be given free of charges or not[54].

That being said, the overarching PSD2 principle on the matter is that where a PSP is allowed to impose charges for "additional or more frequent information" and/or the transmission of information "by means of communication other than those specified in the framework contract", nevertheless the charges shall be "reasonable" and "in line with actual costs" incurred by the PSP (Article 40(3) of PSD2).

In order to avoid that charges applied to PSU for termination of a framework contract could be used as an obstacle to customer mobility and switching of PSP, the principle set out in the PSD2 is that such charges may be applied by PSPs only where the contract is terminated by the consumer less than 6 months after its entry into force. In any case, the charges applied shall be "appropriate and in line" with the costs incurred due to the termination of the contract (Article 55 of PSD2).

Another important issue addressed by the PSD2 regards the "extreme heterogeneity" observed within the EU as to the use, and regulatory treatment thereof, of "surcharging": *i.e.* the much-debated business practice of charging payers for the use of a given payment instrument, typically implemented by merchants so as to steer payers toward their preferred payment instruments. The different approaches followed in the Member

[54] Recital 61 of PSD2.

States on the matter was indeed considered "a source of confusion for consumers, in particular in the e-commerce and cross-border context"[55], and also for the orderly and fair functioning of the internal market.

As a matter of principle, according to Article 62(4) of PSD2 an absolute ban to surcharging is provided for by EU law "only" in case of "use of payment instruments for which interchange fees are regulated under Chapter II" of mentioned Regulation (EU) 2015/751 on card-based payments and "for those payment services to which Regulation (EU) No 260/2012 applies" (*i.e.* credit transfers and direct debits in euro where also other conditions are met).

In all other cases, the PSD2 acknowledges that payee has the right to request "from the payer a charge, offering him a reduction or otherwise steering him towards the use of a given payment instrument" and establishes that the PSPs are prohibited from preventing the payees to do so (Article 62 (3) of PSD2).

However, on one end, the amount of surcharging applied by a payee "shall not exceed the direct costs borne by the payee for the use of the specific payment instrument" (Article 62 (3) of PSD2), on the other is left to Member States the option "to prohibit or limit the right of the payee to request charges taking into account the need to encourage competition and promote the use of efficient payment instruments" (Article 62 (5) of PSD2).

Italy for example, already since the implementation of PSD1[56], has adopted a strict approach to surcharging which has been indeed always prohibited either under Article 3, par. 4, of the Legislative

---

[55] Recital 66 of PSD2.

[56] See Massimo Doria, *Spese Applicabili (commento sub art. 3)*, in AA.VV., *La nuova disciplina dei servizi di pagamento* (Commento al d. lgs. 27 gennaio 2010, n. 11), edited by M. Mancini, M. Rispoli Farina, V. Santoro, A. Sciarrone Alibrandi, O. Troiano, Giappichelli, Torino, 2011, p. 67; Teresa Broggiato, *Profili competitivi e consumeristici del divieto di surcharge*, in Banca d'Italia, *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, cripto valute e rivoluzione digitale*, edited by Fabrizio Maimeri and Marco Mancini, *Quaderni di Ricerca Giuridica della Consulenza Legale*, n. 87, settembre 2019, p. 108.

Decree n. 11/2010[57] on payment services (implementing the PSD1 back then and lately amended to implement the PSD2)[58], and also under Article 62 of the mentioned *Consumer Code*[59].

Besides that, full transparency is anyhow required by the PSD2 as regard information on pricing policies applied for the use of a given payment instrument. Under Article 60 of PSD2, if a payee requests a charge or offers a reduction for the use of a given payment instrument, the payee shall inform the payer thereof in advance, *i.e.* prior to the initiation of the payment transaction (Article 60(1) of PSD2). An obligation of providing information in advance to PSUs also applies to PSPs, or any other party involved in a payment transaction, where they request a charge for the use of a given payment instrument (Article 60(2) of PSD2).

---

[57] Decreto Legislativo 27 gennaio 2010, n. 11, Attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE, 2006/48/CE, e che abroga la direttiva 97/5/CE, see: AA.VV., *La nuova disciplina dei servizi di pagamento* (Commento al d. lgs. 27 gennaio 2010, n. 11), edited by M. Mancini, M. Rispoli Farina, V. Santoro, A. Sciarrone Alibrandi, O. Troiano, Giappichelli, Torino, 2011; Gabriella Gimigliano e Arturo Pironti, *L'attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno: prime osservazioni sul d.lgs. 27 gennaio 2010, n. 11*, in *Contratto e impresa. Europa*, n. 2/2010, p. 700.

[58] Specifically it is therein provided that "a payee shall not charge expenses to a payer with reference to the use of payment instruments"

[59] In particular, according to the *Consumer Code* "merchants shall not impose to consumers, with reference to the use of given payment instruments, any expense for the use of the same instruments, or in cases explicitly established, charges that exceed those incurred by the same merchant". The enforcement of such prohibition in mainly under the responsibility of the Italian Competition Authority that has adopted indeed several enforcement decisions of the matter under article 62 of the *Consumer Code*, see for examples: decision n. 27913 of 18.9.2019 "*Energy – Credit Card Surcharge*", Authority official bulletin n. 40/2019; decision n. 27324 of 13.9.2018 "*Start Romagna – Commissioni Pagamento con Carta di Credito*", Authority official bulletin n. 36/2018; decision n. 26761 of 20.9.2017 "*Edison – Commissioni e Modalità di Pagamento*", Authority official bulletin n. 39/2017; decision n. 26183 of 28.9.2016 "*Norwegian Air Shuttle-Commissioni su carta di credito*" and decision n. 26184 of 28.9.2016 "*Blue Air-Credit card surcharge (CCS)*", Authority official bulletin n. 36/2016.

To strengthen the effectiveness of such obligations, the PSD2 provides that no charges (for the use of a given payment instrument) are due by a payer if the full amount of such charges wasn't made known before the initiation of the payment transaction (Article 60(3) of PSD2).

As to the verification of the compliance with the transparency obligations set forth by the PSD2, the general rule established in Article 41 of PSD2 is that the burden of proof lies with the PSPs, namely is for a PSP "to prove that it has complied with the information requirements" for payment service set out in Title III of PSD2.

That said, to allow an appropriate freedom of business and regulatory flexibility, the PSD2 also establishes that the provisions of its Title III on transparency and information requirements may be waived (in whole or in part) by mutual agreement of the parties when the PSU is not a "consumer" (Article 38 of PSD2).

Furthermore, in line with the principle of proportionality, a set of derogations from information requirements is also directly provided under Article 42 of PSD2 for *low-value payment instruments* and *Electronic money* because such instruments – typically used for on-line or mobile payments – are meant to be "cheap and easy-to-use alternative in the case of low-priced goods and services and should not be overburdened by excessive requirements", but rather be subject to a *lighter regime* as to "information requirements" and "rules on their execution" [60]. For this purpose *low-value payment instruments* are considered those which allow "only individual payment transactions that do not exceed EUR 30 or that either have a spending limit of EUR 150 or store funds that do not exceed EUR 150 at any time" (Article 42(1) PSD2). Nevertheless, in order to cater for national specificities and customs, Member States (or their competent authorities) may "reduce or double" such amounts with regards to *national payment transactions*; for *prepaid payment instruments* Member States may also "increase those amounts up to EUR 50" (Article 42(2) PSD2).

[60] As well as to allow "for the fully integrated straight-through processing of payments", recital 80 of PSD2.

If these conditions and thresholds are met, PSPs are allowed not to provide to PSUs all the detailed "prior general information and conditions" and the "explicit information before execution of individual payment transactions" otherwise mandatory under Articles 51, 52 and 56 of PSD2, but rather to provide the payer "only" with the much more limited set of information and conditions specified in Article 42(1)(a) PSD2[61].

Subject to the agreement of the relevant PSU, it would be also possible for a PSP to derogate from provisions of Article 54 of PSD2, regarding changes to the conditions of the framework contract, and of Articles 57 and 58 on the information to be provided *ex-post* to a payer and/or a payee on individual payment transactions once the transactions are executed[62].

Finally, some other common rules on transparency and information requirements are established for all payment transactions (*i.e.* irrespective of whether they are covered or not by a framework contract) as regards certain aspects of utmost and ever-increasing importance for the transparency of *on-line* and *mobile* payments, namely in the context of cross-border payments and trades executed through *e-commerce* platforms.

First of all, the overarching principles laid down in Article 59 of PSD2 are that "payments shall be made in the currency agreed

[61] Those are indeed only the information "on the main characteristics of the payment service, including the way in which the payment instrument can be used, liability, charges levied and other material information needed to take an informed decision as well as an indication of where any other information and conditions specified in Article 52 are made available in an easily accessible manner".

[62] In particular Article 41(1)(c) of PSD2 provides that "after the execution of a payment transaction: (i) the payment service provider provides or makes available only a reference enabling the payment service user to identify the payment transaction, the amount of the payment transaction, any charges and/or, in the case of several payment transactions of the same kind made to the same payee, information on the total amount and charges for those payment transactions; (ii) the payment service provider is not required to provide or make available information referred to in point (i) if the payment instrument is used anonymously or if the payment service provider is not otherwise technically in a position to provide it. However, the payment service provider shall provide the payer with a possibility to verify the amount of funds stored".

between the parties" (par. 1) and that any *currency conversion service* shall be provided only with the agreement of the payer which shall also receive, from the party offering the currency conversion service, appropriate disclosure of "all charges" and "the exchange rate to be used for converting the payment transaction" (par. 2).

Furthermore, prior to the initiation of a payment transaction, the payee should duly inform the payer if it offers a reduction for the use of a given payment instrument or requests a charge (*i.e.* where surcharging is allowed under Article 62 (4) and (5) PSD2 and national legislation). The same obligation applies to PSPs (or another party involved in a payment transaction) if they request a charge for the use of a given payment instrument. If these *ex ante* transparency obligations are not properly discharged then no charges are due by the payer (Article 60 of PSD2).

Besides such general rules and common provisions on transparency and information requirements, for a number of other aspects Title III of PSD2 establishes a slightly different regulation of single payment transactions covered by a framework contract (Articles 43 – 49 of PSD2)[63], and those not covered by a framework contract (Articles 50 – 58 of PSD2)[64].

In order to avoid pointless and/or redundant regulatory burdens, and to clarify the scope of such different set of rules of Title III of PSD2, Article 43 (2) of PSD2 provides for a principle of

---

[63] Those Articles provide for a specific regulation of : *i)* prior general information; *ii)* information and conditions; *iii)*information for the payer and payee after the initiation of a payment order; *iv)* information for payer's account servicing payment service provider in the event of a payment initiation service; *v)* information for the payer after receipt of the payment order information for the payee after execution.

[64] In this case, the specific provisions regard the following aspects: *i)* prior general information; *ii)* information and conditions; *iii)* accessibility of information and conditions of the framework contract; *iv)* changes in conditions of the framework contract; *v)* termination; *vi)* information before execution of individual payment transactions; *vii)* information for the payer on individual payment transactions; *viii)* information for the payee on individual payment transactions.

simplification and *non-duplication* of information duties regarding single payment transactions where the same information is already given, or will be given, to a PSU on the basis of a framework contract[65].

The implementation in Italy of the PSD2 transparency regime has been completed with the entering into force of the amendments to the Legislative Decree n. 11/2010[66] and the implementing Bank of Italy regulation of 19.2.2019 on the "transparency of banking and financial operations and services – correctness of relationships between intermediaries and their customers"[67].

---

[65] In particular where "a payment order for a single payment transaction is transmitted by a payment instrument covered by a framework contract, the [… PSP …] shall not be obliged to provide or make available information which is already given to the [… PSU …] on the basis of a framework contract with another [… PSP …] or which will be given to him according to that framework contract".

[66] Decreto legislativo 15.12.2017, n. 218, Recepimento della Direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno, che modifica le Direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il Regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, nonché adeguamento delle disposizioni interne al Regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

[67] More precisely, the Bank of Italy regulation of 19.2.2019 implements a number of EU measures, namely: 1) the PSD2; 2) the Directive 2014/17/EU of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010 (so-called: Mortgage Credit Directive – MCD); 3) Directive 2008/48/EC of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/101/EEC (so-called: Consumer Credit Directive – CCD), as amended by Regulation 2016/1011/UE of 8 June 2016 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds and amending Directives 2008/48/EC and 2014/17/EU and Regulation (EU) No 596/2014 (so-called: Benchmark Regulation); 4) EBA's Guide Lines Guidelines on remuneration policies and practices related to the sale and provision of retail banking products and services; 5) ESA's Joint Committee Final Report on guidelines for complaints-handling for the securities (ESMA) and banking (EBA) sectors.

4. The transparency on the terms of execution of payment transactions

In addition to the mentioned rules on transparency of charges, the PSD2 framework is based, more broadly, on the idea that a higher degree of transparency toward PSPs' customers requires also a clearer set of rights and obligations in relation to the provision and use of payment services.

For example, it has been stipulated that, as a matter of principle, in "order to strengthen the trust of consumers [… and allow them access to the information necessary to make their choice …] the use of non-transparent pricing methods should be prohibited, since it is commonly accepted that those methods make it extremely difficult for users to establish the real price of the payment service. Specifically, the use of value dating to the disadvantage of the user should not be permitted"[68].

Detailed rules on the due execution of payment transactions are therefore also laid down in Chapter 3 of Title IV of PSD2, including those regarding the "execution time" and "value date"[69] of payments (Articles 82 – 87 PSD2)[70].

---

[68] Recital 84 of PSD2.

[69] Pursuant to the definition of Article 4 (26) of PSD2, for the purpose of the directive "value date" means a reference time used by a PSP for the calculation of interest on the funds debited from or credited to a payment account.

[70] In particular, pursuant to Article 82 of PSD2 the scope of such detailed rules on execution time and value date apply to 1) "all payment transactions in euro"; 2) "national payment transactions in the currency of the Member State outside the euro area"; 3) "payment transactions involving only one currency conversion between the euro and the currency of a Member State outside the euro area, provided that the required currency conversion is carried out in the Member State outside the euro area concerned and, in the case of cross-border payment transactions, the cross-border transfer takes place in euro". Moreover the same rules apply to payment transactions other the those listed above, "unless otherwise agreed between the payment service user and the payment service provider, with the exception of Article 87, which is not at the disposal of the parties. However, if the payment service user and the payment service provider agree on a longer period than that set in Article 83, for intra-Union payment transactions, that longer period shall not exceed 4 business days following the time of receipt as referred to in Article 78".

These provisions are intended to ensure strong consumers protection in the EU internal market, indeed Article 61 (1) of PSD2 limits the option not to apply some of them[71] (in whole or in part and subject to an agreement between PSPs and PSUs) in those cases where the PSU is not a consumer. Consumers (and other PSUs) are instead allowed to agree on time limits that are different from those laid down in Article 71 of PSD2 for the notification by PSPs to PSUs of unauthorised or incorrectly executed payment transactions giving rise to a claim. Member States have also the option to provide that Article 102 does not apply where the PSU is not a consumer and that provisions of Title IV of PSD2 are applied to microenterprises in the same way as to consumers.

Moreover, irrespective of the nature of the PSU, a list of exceptions and derogations are also established, still subject to an agreement between PSPs and PSUs, for *low-value payment instruments*, *i.e.* payment instruments which "solely concern individual payment transactions not exceeding EUR 30 or which either have a spending limit of EUR 150, or store funds which do not exceed EUR 150 at any time" (Article 63 (1) of PSD2). So as to leave appropriate national flexibility, Member States (or their competent authorities) are anyhow allowed to "reduce or double" any of these amounts and to "increase them for prepaid payment instruments up to EUR 500" (Article 63(2) PSD2).

As regards, the specific rules aiming at enhancing the transparency on the terms of execution of payment transactions, in addition to the mentioned provisions on charges applicable and other steering practices, Article 62 (1) of PSD2 provides that PSPs are in principle also prohibited from charging the PSUs for fulfillment of their "information obligations or corrective and preventive measures" under Title IV of PSD2, unless the possible charging of reasonable, appropriate and cost-oriented fees is instead explicitly allowed by other provisions of PSD2.

In order to ensure due transparency, awareness and "certainty as to the length of time that the execution of a payment order will take [… and …]

[71] Those are the provisions of Article 62(1), Article 64(3), and Articles 72, 74, 76, 77, 80 and 89 of PSD2.

the proper execution of a complete and valid payment order"[72], the PSD2 contains also specific provisions establishing when a payment order should be (legally) considered to have been received (Article 78 of PSD2), and an obligation for the PSPs to notify, if possible, the PSUs "at the earliest opportunity, subject to the requirements of Union and national law"[73] of any refusal to execute a payment order, or to initiate a payment transaction, and of the reason thereof, as well as "the procedure for correcting any factual mistakes that led to the refusal" (Article 79 of PSD2).

For the same purposes, Article 80 of PSD2 also sets forth a "principle of irrevocability" of a payment order, unless otherwise specified therein, once the order has been received by the payer's PSP (*i.e.* the PSU shall not revoke it) or once the payer has given consent to a PISP to initiate the payment transaction or to a payee to execute the payment transaction (Article 80(2) of PSD2).

Such set of clear and transparent cases and deadlines for possible payment order revocation has an increasing importance nowadays because of "the speed with which modern fully automated payment systems process payment transactions, which means that after a certain point in time payment orders cannot be revoked without high manual intervention costs"[74].

Any revocation of a payment order after the provided time limits is allowed only if explicitly agreed between the PSU and the relevant PSPs. The agreement of the payee is also necessary where the payment transaction was initiated by a PISP or by or through the payee. In any case, a revocation based on the agreement of relevant parties should have effects limited to the relationship between a PSU and a PSP, thus be "without prejudice to the irrevocability and finality of payment transactions in payment systems" (recital 78 of PSD2)[75].

---

[72] Recital 77 of PSD2.

[73] Recital 77 of PSD2.

[74] Recital 77 of PSD2.

[75] Moreover such "irrevocability should not affect a payment service provider's rights or obligations under the laws of some Member States, based on the payer's

Revocation is in principle free of charges, as charges for revocation may be applied only if previously agreed in the framework contract (Article 80(2) of PSD2).

Additionally, to ensure full transparency and legal certainty on the amount of funds transferred and received in the context of a payment transaction[76], the PSD2 sets out the principle that the payee shall always receive (*i.e.* credited to its payment account) the full amount of funds transferred by the payer, with consequent obligation for any of the PSPs involved in the execution of a payment transaction, and intermediaries thereof, "to transfer the full amount of the payment transaction and refrain from deducting charges [… or in general to make deductions …] from the amount transferred" (Article 81(1) PSD2).

Deduction of charges from the amount transferred may exceptionally be applied by the PSP of the payee (before crediting the amount transferred to the payee) based on the explicit consent of the payee and only with reference to the PSP's own charges. Should this be the case, to allow the payee to verify that "the amount due is correctly paid"[77] and any possible underlying obligation of the payer is properly fulfilled, the PSP shall ensure full transparency to the payee as to the breakdown of actual amount of funds transferred and the charges in case deducted (Article 81(2) PSD2).

As to the enhanced transparency and efficiency requirements on the "execution time" and "value date" of payments throughout the EU, the fundamental rule established by PSD2 is that in case of payments to be credited to a payment account a "T+1" maximum

framework contract or national laws, regulations, administrative provisions or guidelines, to reimburse the payer with the amount of the executed payment transaction in the event of a dispute between the payer and the payee. Such reimbursement should be considered to be a new payment order. Except for those cases, legal disputes arising within the relationship underlying the payment order should be settled only between the payer and the payee" (recital 79 of PSD2).

[76] As well as to allow "for the fully integrated straight-through processing of payments", recital 80 of PSD2.

[77] Recital 80 of PSD2.

execution time should be respected, meaning that once a payment order is legally deemed to have been received by the payer's PSP (*i.e.* as per Article 78 of PSD2), then the same PSP shall credit the amount of the payment transaction to the account of the payee's PSP "by the end of the following business day".

A limited leeway is granted in case of "paper-initiated payment transactions" for which the "T+1" time limit "may be extended by a further business day" [78], so-called "T+2" rule (Article 83(1) of PSD2)[79].

Once the PSP of the payee has "received" the funds, then the same PSP has in turn to "value date and make available the amount of the payment transaction" to the payment account of the payee in accordance with provisions of Article 87 of PSD2, which is not at the disposal of the parties[80], and whose objective is to avoid that the PSP receiving a payment order in favor of a payee may unduly withhold the funds so received or delay the availability of funds to the same payee.

On the contrary, in case of a payment order initiated by or through the payee (including direct debits and card payments), no statutory execution time is provided in the PSD2, the regulation of the matter is rather left to contractual agreements between the parties (Article 83(3) of PSD2)[81]. However, the PSD2 policy approach is that "in the absence of an explicit agreement between the payment service provider and the payer setting a longer execution time, the same 1-day execution time should apply"[82].

---

[78] The explicit rationale of this different regulatory is "to allow the continued provision of payment services to consumers who are used only to paper documents" (recital 79 of PSD2).

[79] Article 20 of the Italian Legislative Decree 11/2010 implementing some of the provisions of PSD2 establishes that such extension to 2 business days of the time limit for "paper-initiated payment transactions" is subject to the agreement of the parties concerned.

[80] As provided by Article 82 (2) of PSD2.

[81] In particular, the PSP of the payee shall transmit such payment orders to the PSP of the payer by the deadlines explicitly agreed between the payee and the PSP, "enabling settlement, as far as direct debit is concerned, on the agreed due date"

[82] Recital 82 of PSD2.

Such PSD2 rules on execution times are to be intended as a "minimum" harmonization rules, meaning that, pursuant to its Article 86, for "national payment transactions" Member States may maintain or establish rules setting "shorter maximum execution times" (compared to those provided for in Articles 82 – 87 of PDS2) based on the features of relevant payment infrastructures and, for example, "in order to prevent any deterioration in current service levels"[83]. Moreover, in all cases where one of the PSPs "is not located in the Union" the PSD2 provisions on "execution for the full amount and execution time should constitute good practice[84].

In cases where the payee does not have a payment account directly maintained by the PSP "receiving" the funds for the payee, Article 84 of PSD2 provides that this PSP shall make available to the payee the funds so received "within the time limit laid down in Article 83".

In the specific case of cash placed directly on a payment account maintained with a PSP, if no currency conversion is involved, the PSP shall ensure to "consumers" immediate value date and immediate availability of funds once the funds are so placed on the relevant account. Conversely, where the PSU is not a "consumer", a limited delay of value date and availability of cash placed on the account is allowed until the end of the "following business day after receipt of the funds" (Article 85 of PSD2).

Finally, the fundamental policy principles laid down in the PSD2 regarding value date is that value dating practices should be fair and transparent and should not be used to the detriment of the PSUs. For example PSPs should not unduly postpone credit value date or bring forward debit value date compared to the time when the funds are credited or debited on the PSUs' payment accounts. In particular, Article 87 of PSD2 provides that in the ordinary course of business, on one end, the "credit value date" for the payee's payment account should be no later than the business day on which the amount of

[83] Recital 82 of PSD2.

[84] Recital 83 of PSD2.

the payment transaction is credited to the account of the PSP of the payee and, on the contrary, that the "debit value date" for the payer's payment account is no earlier than the time at which the amount of the payment transaction is debited to that payment account. Other specific rules on value dating practices are also set forth in other articles of the PSD2 as for the specific cases regulated therein[85].

The information on the debit and/or credit value dates actually applied are also part of the list of mandatory information concerning the execution of payments to be provided to PSUs according to transparency and information requirements laid down in some articles of PSD2[86].

As to the certainty and transparency of the moment of the availability of funds received via a payment transaction, in principle the PSP of the payee cannot temporarily withhold the funds received on behalf of the payee, unless this could be justified by the need, on the part of the same PSP, to perform a currency conversion between the euro (or a Member State currency) and the currency of a non-EU country. In other words, once a payment to the payee is credited to the payment account of its PSP, then the same PSP shall put the amount of the payment transaction at the immediate disposal of the payee if (on the part of this PSP) no currency conversion is needed or the only currency conversion "is between the euro and a Member State currency or between two Member State currencies". The same obligation applies to payments within one PSP (Article 87 (2) of PSD2).

---

[85] See Article 73 on the PSP's liability for unauthorised payment transactions, Article 76 on the refunds for payment transactions initiated by or through a payee, Article 85 on cash placed on a payment account, Article 89 on PSPs' liability for non-execution, defective or late execution of payment transactions.

[86] Reference is for example to: Article 49 as to data to be provided to a payee immediately after the execution of the payment transaction; Article 57 as to information to be provided to a payer "without undue delay" after the amount of an individual payment transaction is debited from the payer's account or, where the payer does not use a payment account, after receipt of the payment order; Article 58 as to information to be provided to a payee "without undue delay" after the execution of an individual payment transaction.

5. The transparency and security of Internet and mobile payments: Strong Customer Authentication (SCA), dynamic-linking and communication standards.

Another key issue addressed by the PSD2 is the enhancement of security requirements for electronic payments, primarily in order to ensure "the protection of users and the development of a sound environment for e-commerce"[87]. The provisions of PSD2 on the matter are based on the founding principle that all "payment services offered electronically should be carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and to reduce, to the maximum extent possible, the risk of fraud"[88].

Compared to the PSD1, the PSD2 reserves greater and specific attention to payment services offered via Internet, mobile or other *at-distance channels*[89], as so-called electronic *remote payment transactions* (so defined in Article 4(6) of PSD2)[90] are considered generally subject to peculiar and higher risks.

For example, as part of the most debated obligation introduced for PSPs to apply so-called *Strong Customer Authentication* (SCA)[91]

---

[87] Recital 95 of PSD2. As also already stated in a green paper of the European Commission of 2012 the "security of retail payments is a crucial prerequisite for payment users and merchants alike. Consumers are justifiably alerted by frequent press coverage of fraud and data abuse incidents and are therefore particularly sensitive to security issues for card and internet payments. The public consultation on the future of e-commerce in the internal market confirmed this and identified payments security as one of the key hurdles preventing the widespread adoption of electronic commerce", European Commission, Green Paper "Towards an integrated European market for card, internet and mobile payments", Brussels, 11.1.2012 COM(2011) 941 final, p. 18.

[88] Recital 95 of PSD2.

[89] Those are the channels "the functioning of which does not depend on where the device used to initiate the payment transaction or the payment instrument used are physically located", recital 95 of PSD2.

[90] Meaning "a payment transaction initiated via internet or through a device that can be used for distance communication".

[91] For the purpose of PSD2 the SCA means "an authentication based on the use of two or more elements categorised as knowledge (something only the user

(*i.e.* when the payer: *(i)* accesses its payment account online; *(ii)* initiates an electronic payment transaction; *(iii)* carries out any action through a remote channel which may imply a risk of payment fraud or other abuses – Article 97 (1) PSD2) an additional requirement is specifically mandated in case of initiation of *electronic remote payment transactions*, such as e-payments and m-payments.

In the latter case, the PSPs are indeed required to apply a SCA that includes also "elements which dynamically link the transaction to a specific amount and a specific payee", or so-called "dynamic linking". The obligation applies also where payments are initiated through a PISP (Article 97 (2) and (3) PSD2).

However, the requirement to include in the authentication of said *remote transactions* also the use of dynamic codes is to be regarded actually as dual-purposes obligation, *i.e.* it is not a mere additional security measure, but rather also as a peculiar transparency measure.

Indeed, at a closer analysis it results that the rationale of such obligation is primarily "to make the user aware, at all times, of the amount and the payee of the transaction that the user is authorizing"[92], including at the very moment when the user is initiating the transaction.

In this respect, it's important to note that the regulatory framework of PSD2 on the matter is supplemented and complemented, as for many other important technical aspects of PSD2[93], by Regulatory Technical

---

knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data", Article 4 (30) of PSD2.

[92] Recital 95 of PSD2.

[93] For example, as highlighted by the EBA, in order to support the objectives of PSD2, "namely enhancing competition, facilitating innovation, protecting consumers, increasing security and contributing to a single EU market in retail payments, the [… PSD2 …] gave the EBA the task of developing 12 technical standards and guidelines to specify detailed provisions in relation to payment security, authorisation, passporting, supervision and more", Opinion of the European Banking Authority on the elements of strong customer authentication under PSD, EBA-Op-2019-06, 21 June 2019, paragraph 2.

Standards (RTS) to be developed by the European Banking Authority (EBA), in cooperation with the European Central Bank, and legally adopted by the European Commission (Article 98(1)(a) of PSD2).

The RTS specifying the requirements of the SCA has been lately adopted by the European Commission Delegated Regulation (EU) 2018/389 of 27.11.2017 (SCA Regulation)[94], it establishes detailed rules and a set of strict security requirements also as to the correct implementation of *dynamic linking* which are intended to remain, at least in principle, technologically neutral[95].

Specifically, where PSPs apply the SCA to the initiation of *electronic remote payment transactions* (in accordance with Article 97(2) of PSD2) they shall also meet each of the following supplementary requirements: *i)* "the payer is made aware of the amount of the payment transaction and of the payee"; *ii)* "the authentication code generated is specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction"[96]; *iii)* "the authentication code accepted by the [… PSP …] corresponds to the original specific

[94] Commission delegated regulation (EU) 2018/389 of 27.11.2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

[95] As specified in recital 4 of the SCA Regulation, "a specific technology for the implementation of authentication codes should not be required. Therefore authentication codes should be based on solutions such as generating and validating one-time passwords, digital signatures or other cryptographically underpinned validity assertions using keys or cryptographic material stored in the authentication elements, as long as the security requirements are fulfilled".

[96] In order to meet this requirement is also specifically established that in case of "card-based payment transaction for which the payer has given consent to the exact amount of the funds to be blocked pursuant to Article 75(1) of [… the PSD2 …], the authentication code shall be specific to the amount that the payer has given consent to be blocked and agreed to by the payer when initiating the transaction". On the contrary when "the payer has given consent to execute a batch of remote electronic payment transactions to one or several payees, the authentication code shall be specific to the total amount of the batch of payment transactions and to the specified payees" (Article 5(3) of SCA Regulation).

amount of the payment transaction and to the identity of the payee agreed to by the payer"; *iv)* "any change to the amount or the payee results in the invalidation of the authentication code generated" (Article 5(1) of the SCA Regulation). Moreover, PSP are mandated to "ensure the confidentiality, authenticity and integrity" of (i) "the amount of the transaction and the payee throughout all of the phases of the authentication" and (ii) "the information displayed to the payer throughout all of the phases of the authentication including the generation, transmission and use of the authentication code" (Article 5(2) of SCA Regulation).

The content of such technical rules as to the implementation of the *dynamic linking* confirms the previously mentioned dual-purposes nature of this regulatory requirement, *i.e.* the security of payments by ensuring full transparency and certainty, in favor of the PSUs, as to the specific amount of a payment transaction and the identity of the payee also at the very moment of the initiation of an *electronic remote payment transaction* and throughout all of the phases of its authentication.

That said, in order to ensure a balanced and proportionate regulatory approach, the SCA Regulation also provides for a list of exemptions from the obligations to apply the SCA which are essentially dependent on "the level of risk, amount, recurrence and the payment channel used for the execution of the payment transaction"[97].

As regards the initiation of *remote electronic payment transaction*, explicit exemptions are provided for when the payer initiates a *low-value* transaction (pursuant to Article 16 of the SCA Regulation)[98],

[97] Recital 9 of the SCA Regulation.

[98] A remote electronic payment transaction can be considered as low-value transaction exempted from the obligation of the SCA if the amount of the remote electronic payment transaction does not exceed EUR 30 and (i) the cumulative amount of previous remote electronic payment transactions initiated by the payer since the last application of strong customer authentication does not exceed EUR 100 or (ii) the number of previous remote electronic payment transactions initiated by the payer since the last application of strong customer authentication does not exceed five consecutive individual remote electronic payment transactions.

or when the payer initiates a *low-risk* transaction, identified as such by the same PSP according to its own *transaction risk analysis* conducted in compliance with the much detailed provisions of Articles 18, 19, 20 and 21 of the SCA Regulation.

Chapter V of the SCA Regulation aims instead at establishing "common and secure open standards for the communication" between ASPSPs, PISPS, AIPSPs, payers, payees and other PSPs "in relation to the provision and use of payment services in application of Title IV" of PSD2 (Article 1(d) of the SCA Regulation).

Nevertheless, it could be observed that some of such requirements for communication absolve also the function of increasing the transparency of online and mobile payments, as they namely provide for:

(i) the secure identification of the parties involved in electronic payments (Article 28 of SCA Regulation)[99];

(ii) the traceability of all payment transactions and other interactions of the PSPs with third-parties (including the PSU, PSPs and merchants) in the context of the provision of the payment service and the *ex post* knowableness of all events relevant to the electronic transaction in all the various stages (Article 29(1) of SCA Regulation)[100].

[99] In particular PSPs are mandated "ensure secure identification when communicating between the payer's device and the payee's acceptance devices for electronic payments, including but not limited to payment terminals" and also to "ensure that the risks of misdirection of communication to unauthorised parties in mobile applications and other payment services users' interfaces offering electronic payment services are effectively mitigated".

[100] Specifically, for the purpose of traceability and *ex post* knowledge, PSPs are required to "ensure that any communication session established with the payment services user, other payment service providers and other entities, including merchants, relies on each of the following: (a) a unique identifier of the session; (b) security mechanisms for the detailed logging of the transaction, including transaction number, timestamps and all relevant transaction data; (c) timestamps which shall be based on a unified time-reference system and which shall be synchronised according to an official time signal".

Finally, it is worth recalling that pursuant to Article 74 (2) of PSD2 where the PSP of the payer does not require SCA then "the payer shall not bear any financial losses unless the payer has acted fraudulently"[101], furthermore, where the payee, or its PSP, fails to accept SCA, "it shall refund the financial damage caused to the payer's payment service provider".

The same liability regime applies also when a PSP applies one the exemptions to the SCA set out in the SCA Regulation. It follows that opting for the application of an exemption to SCA is basically at the risk and expenses of the PSP of the payer.

The Article 39 of the SCA Regulation provides that the same Regulation applies "from 14 September 2019", save for "paragraphs 3 and 5 of Article 30" which applies from 14 March 2019. Therefore also the requirements of the SCA and "dynamic linking" should have been applied and complied with from 14 September 2019.

Nevertheless, the very detailed legal framework established by PSD2 and relating Delegated acts results to be somehow too much rule-based and prescriptive, so giving rise to numerous issues as to its correct and harmonized implementation. This triggered the need for the EBA to play an active role[102] and intervene frequently so as to ensure a common

---

[101] It implies that, if the payer's PSP does not require SCA, in case of unauthorised payment transactions no losses should be borne by the payer even if the payer failed to fulfil one or more of its obligations under Article 69 of PSD2 with gross negligence.

[102] Pursuant to Article 29 of Regulation (EU) No 1093/2010 of the European parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC, the EBA "shall play an active role in building a common Union supervisory culture and consistent supervisory practices, as well as in ensuring uniform procedures and consistent approaches throughout the Union. The Authority shall carry out, at a minimum, the following activities: (a) providing opinions to competent authorities; (b) promoting an effective bilateral and multilateral exchange of information between competent authorities, with full respect for the applicable confidentiality and data protection provisions provided for in the relevant Union legislation; (c) contributing to developing high-quality and uniform supervisory standards, including reporting standards, and international accounting standards

EU approach to the application of PSD2 regulatory framework by publishing formal opinions[103], guidelines[104] and a vast number of Q&As[105] which have increasingly become a kind of informal source of EU law on the matter, so making the resulting regulatory framework even more complex, multi-layered and detailed though.

For example, in its latest opinions on the correct implementation of the SCA requirements under the PSD2, the EBA acknowledged that certain issues and concerns exist regarding the state of preparedness of some actors in the payment services value-chain to the new SCA requirements, primarily with regard to e-commerce merchants[106].

Consequently, the EBA communicated that "on an exceptional basis and in order to avoid unintended negative consequences for some payment service users after 14 September 2019"[107], a certain supervisory flexibility may be allowed at national level, specifically in order "to provide limited additional time to allow issuers to migrate to authentication approaches that are compliant with SCA […] and

---

in accordance with Article 1(3); (d) reviewing the application of the relevant regulatory and implementing technical standards adopted by the Commission, and of the guidelines and recommendations issued by the Authority and proposing amendments where appropriate; and (e) establishing sectoral and cross-sectoral training programmes, facilitating personnel exchanges and encouraging competent authorities to intensify the use of secondment schemes and other tools. 2. The Authority may, as appropriate, develop new practical instruments and convergence tools to promote common supervisory approaches and practices".

[103] See for example: EBA Final report "Guidelines on the conditions to benefit from an exemption from the contingency mechanism under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC), EBA/GL/2018/07 4 December 2018; EBA Opinion on the implementation of the RTS on SCA and CSC, EBA-Op-2018-04, 13.6.2018.

[104] See for example the EBA's opinion on the transition from PSD1 to PSD2, EBA/Op/2017/16, 19.12.2017.

[105] https://eba.europa.eu/single-rule-book-qa.

[106] EBA opinion on the deadline for the migration to SCA for e-commerce card-based payment transactions, EBA-Op-2019-11, 16.10.2019, para 2.

[107] EBA opinion on the elements of strong customer authentication under PSD, EBA-Op-2019-06, 21.6.2019, para 13.

acquirers to migrate their merchants to solutions that support SCA"[108]. The scope of this flexibility has been lately more precisely restricted to "e-commerce card-based payment transactions" only and consequently to "card-issuing PSPs"[109]. In order to benefit from such *moratorium* the interested "PSPs have to "set up a migration plan", agree the plan with their National Competent Authorities and "execute the plan in an expedited manner"[110]. To ensure full transparency and information to PSUs, PSPs should also "have customer communication plans in place, including for the end customers of the merchants"[111].

Following a fact-finding exercise carried out over summer 2019, the EBA has lately communicated that "migration plans of PSPs, including the implementation and testing by merchants, should be completed"[112] by 31.12.2020. In Italy, the policy stance of the Bank of Italy has been to apply such *moratorium* consistently with the EBA's recommendations[113].

To conclude, it is important to clarify that such supervisory flexibility has to be intended, specifically and solely, as an *enforcement moratorium*, meaning that during the allowed migration period the competent Authorities "would not take enforcement/sanction actions against PSPs if they respect" the conditions provided[114], however the application date of PSD2 rules on SCA requirements remains unaffected, and therefore they fully apply as of 14.9.2019.

---

[108] EBA opinion on the elements of strong customer authentication under PSD, EBA-Op-2019-06, 21.6.2019, para 13.

[109] EBA opinion on the deadline for the migration to SCA for e-commerce card-based payment transactions, EBA-Op-2019-11, 16.10.2019, para 3.

[110] EBA opinion on the elements of strong customer authentication under PSD, EBA-Op-2019-06, 21.6.2019, para 13.

[111] EBA opinion on the elements of strong customer authentication under PSD, EBA-Op-2019-06, 21.6.2019, para 14.

[112] EBA opinion on the deadline for the migration to SCA for e-commerce card-based payment transactions, EBA-Op-2019-11, 16.10.2019, para 13.

[113] Bank of Italy press releases of 1.8.2019 and 29.11.2019.

[114] EBA opinion on the deadline for the migration to SCA for e-commerce card-based payment transactions, EBA-Op-2019-11, 16.10.2019, para 10.

This implies that also the application date of PSD2 rules on the liability regime for unauthorised payment transactions remains the 14.9.2019, including those of Article 74(2) PSD2, thus providing a further incentive for PSPs to migrate with no undue delay to "SCA-compliant solutions and approaches"[115].

Riferimenti bibliografici

AA.VV., *La nuova disciplina dei servizi di pagamento* (Commento al d. lgs. 27 gennaio 2010, n. 11), *edited by* M. Mancini, M. Rispoli Farina, V. Santoro, A. Sciarrone Alibrandi, O. Troiano, Giappichelli, Torino, 2011.

Bank for International Settlements and Financial Stability Board, *FinTech credit. Market structure, business models and financial stability implications. Report by a Working Group established by the Committee on the Global Financial System (CGFS) and the Financial Stability Board (FSB)*, 22.5.2017.

Broggiato Teresa, *Profili competitivi e consumeristici del divieto di surcharge*, in AA.VV., *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, cripto valute e rivoluzione digitale, edited by* F. Maimeri and M. Mancini, Banca d'Italia, *Quaderni di Ricerca Giuridica della Consulenza Legale*, n. 87, settembre 2019.

De Stasio Vincenzo, *Operazioni di pagamento non autorizzate e restituzione*, Educatt, Milano, 2013.

Doria Massimo, *Spese Applicabili (commento sub art. 3)*, in AA.VV., *La nuova disciplina dei servizi di pagamento. (Commento al d. lgs. 27 gennaio 2010, n. 11)*, *edited by* M. Mancini, M. Rispoli Farina, V. Santoro, A. Sciarrone Alibrandi, O. Troiano, Giappichelli, Torino, 2011.

European Banking Authority, *Opinion on the deadline for the migration to SCA for e-commerce card-based payment transactions*, EBA-Op-2019-11, 16.10.2019.

European Banking Authority, *Opinion on the implementation of the RTS on SCA and CSC*, EBA-Op-2018-04, 13 June 2018.

[115] EBA opinion on the deadline for the migration to SCA for e-commerce card-based payment transactions, EBA-Op-2019-11, 16.10.2019, para 11.

European Banking Authority, *Opinion on the elements of strong customer authentication under PSD*2, EBA-Op-2019-06, 21.6.2019.

European Commission, *Green Paper "Towards an integrated European market for card, internet and mobile payments"*, Brussels, 11.1.2012 COM(2011) 941 *final*.

Gammaldi Domenico – Iacomini Costanza, *Mutamenti del mercato dopo la PSD2*, in AA.VV., *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, cripto valute e rivoluzione digitale, edited by* F. Maimeri and M. Mancini, Banca d'Italia, *Quaderni di Ricerca Giuridica della Consulenza Legale*, n. 87, settembre 2019.

Gimigliano Gabriella e Pironti Arturo, *L'attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno: prime osservazioni sul d.lgs. 27 gennaio 2010, n. 11*, in *Contratto e impresa. Europa*, n. 2/2010.

Lemma Valerio, *FinTech Regulation. Exploring New Challenges of the Capital Markets Union*, Palgrave Macmillan, 2020.

Maimeri Fabrizio, *La disciplina dei costi e delle commissioni interbancarie nella PSD2*, in AA.VV., *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, cripto valute e rivoluzione digitale*, edited by F. Maimeri and M. Mancini, Banca d'Italia, *Quaderni di Ricerca Giuridica della Consulenza Legale*, n. 87, settembre 2019.

Menzella Raffaella, *Il ruolo dei big data e il mobile payment*, in AA.VV., *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, cripto valute e rivoluzione digitale*, *edited by* F. Maimeri and M. Mancini, Banca d'Italia*, Quaderni di Ricerca Giuridica della Consulenza Legale*, n. 87, settembre 2019.

Mezzacapo Simone, *La* vexata quaestio *della qualificazione della fattispecie giuridica di "conto di pagamento" ai sensi e per gli effetti della diritto UE dei servizi di pagamento nel "mercato interno"*, in *Diritto della Banca e del Mercato Finanziario*, n. 4/2019.

Mezzacapo Simone, *Competition policy issues in EU retail payment business: the new PSD 2 regulatory principle of open on-line access to information from "payment accounts" and associated "payment transactions"*, in *European Competition Law Review*, Vol. 39, Issue 12, 2018.

Mezzacapo Simone, *La nuova disciplina nazionale dei "conti di pagamento" alla luce dell'armonizzazione attuata con la Payment Accounts Directive*, in *Banca Borsa e Titoli di Credito*, n. 6/2017.

Mezzacapo Simone, *La nuova disciplina UE dei limiti alle interchange fees e delle business rules in materia di "pagamenti basati su carte", tra regolamentazione strutturale del mercato interno e promozione della concorrenza*, in *Diritto della banca e del mercato finanziario*, n. 3/2017.

Moliterni Francesco, *I sistemi di pagamento informali fra rimesse di denaro e contratto di rete*, Giuffrè, Milano, 2019.

Porta Fabio, *Obiettivi e strumenti della PSD2*, in AA.VV., *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, cripto valute e rivoluzione digitale*, *edited by* F. Maimeri and M. Mancini, Banca d'Italia*, Quaderni di Ricerca Giuridica della Consulenza Legale*, n. 87, settembre 2019.

Sciarrone Alibrandi Antonella, *L'adempimento dell'obbligazione pecuniaria tra diritto vivente e portata regolatoria indiretta della Payment services directive 2007/64/CE*, in AA.VV., *Il nuovo quadro normativo comunitario dei servizi di pagamento. Prime riflessioni*, edited by M. Mancini e M. Perassi, Banca d'Italia, *Quaderni di Ricerca Giuridica della Consulenza Legale*, n. 63, Dicembre 2008.

Santoro Vittorio, *I servizi di pagamento*, in *Ianus*, n. 6/2012.

Ugo Minneci
(Università degli Studi di Milano)

UNAUTHORIZED PAYMENT TRANSACTIONS ACCORDING TO PSD 2 ENFORCEMENT: FROM THE BANKING AND FINANCIAL OMBUDSMAN TO CASE-LAW

1. Introduction

The decisions taken in this area by courts of law can barely be counted on one hand and, moreover, when it comes to decisions of the higher courts, these often stem from events occurred even before the implementation of the PSD1. Conversely, not only is there a considerable range of Banking And Financial Ombudsman decisions regarding payment instruments; due to the ease of access to this ADR (Alternative Dispute Resolution) system, the time lag between the occurrence of the challenged transaction and the onset of the decision thereon, is extremely reduced, so much so that a fair number of cases resolved in light of the PSD2 are already recorded today. In view of this, it does not seem hazardous to state that, in the area of payment services, the decisions of the Banking And Financial Ombudsman represent the "prevailing standard" in this regard.

2. Preliminary remarks

2.1. Payment transactions (in particular, the transfer of funds without material money being delivered) are covered by specific EU regulations (first the PSD 1 Directive, then PSD 2), representing a special category, if not a stand-alone one, nevertheless boasting a

range of specific rules[1]. In pursuing the aim of ensuring the efficiency and security of the European payments system, this legislation construes the payment transaction as a procedure[2], offering a number of solutions to specific issues, according to the pragmatic approach of the EU lawmaker. Hence, the warning of several experts to carefully consider the traceability of the case within traditional schemes or figures.

2.2. Barring minor cases, the provision of payment services takes place on the basis of a framework contract signed between the financial intermediary and the client (the user of the service). This agreement, as far as the service provider is concerned, can be classified as a "business agreement" according to the definition of Arturo Dalmartello[3]: an agreement representing the activity carried out by the financial intermediary[4].

2.3. The finding of being dealing with an ephemeral situation, being both an agreement and a business transaction, is not in itself irrelevant. Indeed, it offers an important key to capturing the meaning of the solutions adopted by the lawmaker, as well as to regulate and manage any gaps or inconsistencies in the legal framework. In other words, the connection resulting from the fact that, for one of the parties, the service provided in the contract falls within the scope of an activity carried out in an organized and permanent manner, can be regulated and managed according to different reasoning schemes and perspectives compared to an agreement that, for both parties, is structured as occasional services or, in any case, unrelated to the professional or entrepreneurial activity of the same parties.

---

[1] For an in-depth examination of the regulations on the subject, see V. SANTORO, *I servizi di pagamento*, in Ianus, 2012, 7 seq.

[2] Resort to the category of the procedure to explain the string of stages in which the execution of a payment transaction unfolds, is made by V. DE STASIO, *Ordine di pagamento non autorizzato e restituzione della moneta*, Milan, 2016.

[3] A. DALMARTELLO, *Contratti d'impresa,* in *Enc. giur.,* IX, Roma, 1988.

[4] The perspective of the business contract as a key to determine the risk-sharing criteria within the provision of payment services in U. MALVAGNA, *Clausole di riaddebito e servizi di pagamento*, Milan, 2018.

2.4. In the overall understanding of the regulations on the subject and, in particular, in the grounds for the criteria for sharing the risks linked to the pathologies that can occur in the execution of the relevant transactions, the further fact that, in today' scenario, recourse to intermediation in payments is becoming an ever more often required solution, rather than the result of a free choice, cannot be disregarded, given the implementation of a regulatory trend aimed at discouraging the use of cash.

3. The regime of unauthorized transactions in the light of Legislative Decree no. 11 dated January 27th, 2010 (and subsequent amendments)

3.1. A transaction is deemed to be disallowed if the client disowns it within 13 months of the debit date (art. 9, paragraph 1). Reasons for the disavowal can be many: just to mention the most frequent ones, in case of online transfer, not having actually carried out the same; in case of withdrawal at the ATM, the theft or misappropriation of the bank card.

Without prejudice to the fact that, once the blocking of the instrument has been requested, no subsequent operation can be debited to the client, except in the case of fraud (art. 12, paragraph 1), it is worth noting from the outset that the regulations on the subject also allow for the repudiation of payments previously made: this without any particular charges of notification, other than the request to disavow the operation that would have given rise to the debit.

3.2. Article 10 outlines a specific set of rules for this situation, as recently stated by the Banking And Financial Ombudsman Coordinating Panel[5], which consists of two steps.

[5] See Coordinating Panel, Decision No. 22745, October 10th, 2019.

3.3. In order to maintain the charge in the hands of the client, firstly, the intermediary must provide suitable evidence proving the authenticity of the disputed transaction, its correct registration and accounting, and the non-occurrence of the effects of the malfunctioning of the procedures necessary for its execution or any other mishap (art. 10, paragraph 1). The bank is required to prove its correct handling (better, processing) of the transaction, adopting conduct and/or procedures that comply with industry standards.

It is worth pointing out that, to meet the burden of proof relating to the correct authentication, the Banking And Financial Ombudsman panels require the production of the so-called logs, i.e. the IT records, taken from the centralized data base systems, enabling the reconstruction of the transaction processing procedure from the starting point to its conclusion.

In the event of failure to provide the required proof, the amount debited is re-credited without the need for further investigation.

3.4. However, it should be pointed out that, since the activity of a professional subject is at stake (not by chance, a business agreement has been mentioned), the service provided by the intermediary will be assessed pursuant to the standards set out in art. 1176, paragraph 2 of the Italian Civil Code: i.e. according to standards of due diligence, or – as specified by Italian Supreme Court ruling 9158/2018 – on the basis of the technical diligence standard adopted by the prudent banker.

Rather, the provision to place on the bank the burden of proving the correct execution of the transaction ordered by the customer is definitely in line with the general principles governing compliance.

With regard to the allocation of the burden of proof in terms of liability, once evidence of the source of the contractual or legal entitlement has been provided and, if applicable, of the expiry date, the creditor can merely allege (without proving it) the non-fulfillment (or inexact fulfillment) of the counterparty, with the latter, on the other hand, bearing the burden of proving to have

complied with (or to have exactly fulfilled the service due), or that the non-fulfillment or non-performance is due to a non-attributable impossibility[6].

A divergence from the general principles of the law applied in terms of responsibility for non-fulfillment lies in the very fact that the client has such a light burden of proof: as already mentioned, a simple disavowal on its part is enough.

Actually, in the case of a dispute over faulty performance (the case of an unauthorized payment), although the creditor is exempted from demonstrating the inaccuracy of the service received, nevertheless, there is a general trend to exclude that the latter's objection can be limited to a generic reproach of having performed badly: rather, a somehow circumstantial statement, or rather characterized by a certain degree of detail, is required, so as to ensure the principle of cross-examination, namely the possibility for the debtor to deal with specific charges[7].

The solution provided by Art. 10 deserves nevertheless to be approved: both as it would be rather difficult for an individual to even hypothesize the reasons that led to the execution of an unauthorized transaction, given the extreme technical complexity that characterizes today's payment systems; and because the possibility of the most immediate access possible to the investigation of any anomalies that may have affected the actions of the intermediary – even at the risk of favoring opportunistic behavior on the part of the client – is an essential condition for achieving the basic option pursued by European and domestic lawmakers (the latter also through the introduction of actual limits through the provision of monetary pieces) of establishing a proactive environment with respect to a widespread and extensive use of payment instruments other than cash.

---

[6] See among the others Supreme Court May 21st, 2019, No. 13685..

[7] For example, it is well known that, during the corporate liability proceedings against directors of companies, the law usually requires (at least) the indication of the alleged episodes of mismanagement; likewise, when the bad execution of an operation is challenged, the reasons for the non-compliance or the faults charged cannot be ignored.

3.5. As already mentioned, the bank's fulfillment of the burden of proof just referred to, is not sufficient to definitively close the case, acting as a necessary condition, but not yet sufficient, for the transaction to be considered definitively attributable to the client.

The intermediary is also required – pursuant to the last paragraph of art. 10, last paragraph, – to prove the further element (if not intent or fraud, at least) of the user's gross negligence (i.e. the existence of abnormal, conduct on the part of the client). Indeed, in the absence of such proof, the transaction will not be counted against the customer, except for the possibility of an exemption of € 50.00 in the event of theft, loss or misappropriation of the payment instrument.

On closer examination, this is the main and perhaps most significant divergence from the general principles of responsibility for non-fulfillment and, in particular, from the provisions of art. 1227 of the Italian Civil Code.

On the other hand, the practical result of charging the intermediary also with the risk of the client' slight negligence – though at first glance unsettling in terms of common sense – ends up losing its (seemingly) "subversive" value, should the gaze be raised beyond the limited horizon of the single transaction to frame everything in the perspective of the business activity: once again representing a solution to indirectly encourage the use of instruments other than cash.

3.6. That said, the Banking And Financial Ombudsman Panels, to prove the gross negligence of the client, also admit recourse to presumptions; even if a steady hardening in this regard must be recorded – especially since the introduction of PSD 2.

In detail, there is still the opinion that, in the hypothesis of theft and/or loss of the ATM card, the assessment of an absolutely close time span between the loss of the availability of the "plastic" card and the completion of the first challenged transaction would be worth demonstrating, already in itself, a seriously negligent attitude

on the part of the user in the safekeeping of the payment instrument, leading to the presumption of the retention, together with the latter, of the related login credentials[8].

In terms of online payments, however, a degree of evolution has taken place. Faced with the adoption by the intermediary of a twofold security factor system (for example, a system using a static credential in combination with an otp password), in the past the Panels were used to assume – unless conflicting circumstances were to arise from the documents in hand – that the client was liable for gross negligence in the form of a phishing incident or, in any case, of having recklessly communicated to third parties the codes for using the tool.

Nowadays, with the raising of the strong authentication process as protection imposed by the law (as such, in the event of non-adoption, likely to reflect an organizational deficiency falling within the scope of paragraph 1 of art. 10), in order to support the allegation in question, something else is also required.

More in detail, since the idea of a sort of automation between the use of a two-factor system by the intermediary and a serious fault of the client in the safekeeping of the identification codes and the OTP device has been discarded – also as a result of the provisions of art. 10, paragraph 2, which specifies that the monitoring on the use of the proper credentials cannot be considered in itself sufficient to prove gross negligence on the part of the customer[9] –, the basis

[8] Among the many others see Banking and Financial Ombudsman's Milan Panel, decision dated September 2nd, 2020, no. 15330.

[9] See Banking and Financial Ombudsman Coordinating Panel, Decision No. 22745 dated October 10, 2019, which states that "the provision in Art. 10, paragraph 2 with regard to the burden placed on the PSP of proof of fraud, intent and gross negligence of the user should be interpreted in the sense that the document output aimed at proving the authentication and formal regularity of the disputed transaction does not satisfy, in itself, the probative burden, since it is necessary that the intermediary specifically provides to indicate a set of elements that characterize the mode of execution of the transaction from which evidence can be drawn, presumptively, of the gross negligence of the user".

of the allegation can be found (after careful consideration of the various circumstances of the case) in further elements, such as, on the one hand, the particular technical reliability of the instrument and/or the absence of anomalies in the order, on the other hand, the evidence of particularly negligent conduct of the user such as the refusal to use the SMS alert service, even if offered free of charge, or the failure to check the account for a lengthy period of time[10].

4. Contributory negligence

4.1. A particular focus should be placed on cases where both parties are negligent. This could be, for example, the case of a particularly naive conduct client-side (for example, the fact of having taken the bait of a phishing email), and the adoption of inadequate security measures, as not (at least completely) in line with industry standards, intermediary-side.

In such cases, the structural imbalance between the contracting parties, in the assessment of the Banking And Financial Ombudsman Panels, is likely to arise, with the consequence of attributing – beyond the seriousness of the conduct of the user – a weight which, if not completely overwhelming, is nevertheless relevant to the negligence of the intermediary.

This is not so much an immediate result of the specific regulations on the subject, but more generally a consequence of the "business" qualification of the agreement regarding the offer of payment services. In fact, it would be against common sense even more than law not to perceive the qualitative rather than quantitative discrepancy between the negligence attributable to the insider with respect to the contractual service and the fault attributable to the client who uses the service as an outsider.

[10] See Banking and Financial Ombudsman's Milan Panel decision Aug. 25th, 2020, No. 14804; and decision Sept. 3rd, 2020, No. 15392.

4.2. That said, the case history offers at least three types of situations, where Banking And Financial Ombudsman Panels are likely to recognize a contributory negligence on the part of the intermediary that can burden the latter with all or part of the economic responsibility for the challenged transactions, regardless of the seriousness of the user's negligence.

The first concerns the Bank failure to intervene when faced with one of the cases (so-called indexes) of risk of fraud identified by art. 8 of Ministerial Decree no. 112 dated April 30th, 2007.

Although conceived with specific regard to the use of payment cards, the Banking and Financial Ombudsman's cases have a broader value[11] considering them to be representative of anomalies and/or fraud patterns which cannot but be perceived by a security system meeting the required efficiency standards. This leads to the implicit consequence of deeming the intermediary's organisational deficiency to be significant in any case, resulting in the intermediary being charged for the amount of the transactions carried out in the time following that in which a responsive approach by the intermediary could reasonably have been expected (such as the blocking of the instrument operativity together with an interaction with the client).

4.3. Another event likely to give rise to a case of contributory negligence is linked to the failure by the intermediary to forward an SMS alert (or any other equivalent) to the client, where contractually provided for. In fact, even in cases of serious negligence on the part of the user, the finding of failure to send the text message can lead to a sort of overall reinterpretation of the case, with the possibility of charging the intermediary (in whole or in part) for the amount of the disputed transactions subsequent to the first one[12].

---

[11] See Milan Panel, decision dated February 5th, 2020, no. 1725.

[12] In the opinion of the Coordinating Panel (decision November 6th, 2019, no. 24366), it must be considered that among the duties of protection of the user borne by the intermediary, falls the burden of providing the SMS alert service or

4.4. Lastly, the so-called sim swap fraud problem can be mentioned. This is a type of fraud that can occur when the user is legitimated to authenticate payment transactions also through an OTP sent to his cell phone via SMS. In order to carry out this type of fraud, the offenders must i) acquire the data and credentials of the victim's home banking through social engineering techniques and phishing activities; ii) request a new sim card from the phone provider, also using forged documents, pretending to have lost or destroyed the previous one; iii) obtain from the victim's bank, through the use of the same phone number, authorization to operate on the victim's online account.

As can easily be guessed, this is a rather sophisticated case, which undoubtedly bears witness to the client's carelessness in revealing access codes, but which also highlights a criticality in the organization of the service set up by the intermediary for not having adopted suitable precautions against the risk that the SIM card used for authentication may be fraudulently replaced, thus nullifying the security devices adopted to protect the client.

For this reason, even in the face of a fraud that starts from an episode of phishing, the Banking And Financial Ombudsman Panels are in favor of recognizing – at least – a situation of contributory negligence[13], such as to allow the economic burden of the disowned transactions to be shared between the intermediary and the user[14].

---

similar, the intermediary can only be exonerated by demonstrating the explicit refusal of the user to use it. For the consideration of the failure to promptly send an SMS alert as indicative of a fault on the part of the intermediary relevant for the purposes of art. 1227 of the Civil Code, see Banking and Financial Ombudsman Milan Panel, decision dated September 2nd, 2020, no. 15939.

[13] See Banking and Financial Ombudsman Coordinating Panel, Decision No. 14213, August 13th, 2020.

[14] In some cases, the organisational deficiency was considered so serious that the burden of proof required by paragraph 1 of art. 10 was not considered to have been met: see Banking and Financial Ombudsman Bologna Panel, decision no. 14765 dated August 25th, 2020.

THIRD PART

THE TRANSPOSITION OF PSD2: THE ROLE OF EBA AND THE NATIONAL RULEMAKERS

Dimitrios Linardatos[1*]
(University Mannheim)

THE TRANSPOSITION OF THE PSD 2: THE ROLE OF EBA AND OF THE NATIONAL LEGISLATOR IN GERMANY

This paper seeks to provide an overview of the implementation of the second Payment Services Directive (PSD 2)[2] into German law. Its structure reflects the topics discussed in the panel at the Bergamo Conference on "The Transposition of the PSD 2 and Open Banking" and the course of my presentation held at the conference. The first part deals with the role of the European Banking Authority (EBA) within the process of transposing the PSD 2 into national law. The second part presents the basic structure of the Payment Services Law regime in Germany. In the third part, I will discuss one specific amendment of the PSD 2 which refers to requirements on evidence on authentication and execution of payment transactions. The fourth part considers the regulatory decisions of the German legislator concerning the so-called Third Party Service Provider (TPP). In the following fifth part, I outline the requirements on Strong Customer Authentication (SCA) as defined in German Law.

[1*] Post-Doc (Habilitand) at the Chair of Prof. *Dr. Georg Bitter* (University Mannheim) and Lecturer at the Mannheim Business School (Commercial and Capital Markets Law). The author is grateful for numerous comments and suggestions from *Sebastian Seidel* (Mannheim and Amsterdam).

[2] 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.

The sixth part will shed some light onto the difficult relationship between the General Data Protection Regulation (GDPR) and the PSD 2. Finally, the paper will close with an overall assessment of the PSD's transposition into German law.

1. The prominence of the EBA

As the title indicates, one of the topics discussed at the conference was EBA's role within the process of implementing European Directives into national law. With respect to Germany, the legal situation is clear: announcements and opinions of the EBA do not directly affect the implementation of the Directive, given that the EBA has no legislative power. That is not to say that the German legislator does not take EBA's comments on the interpretation of a Directive into account. It is also acknowledged in Germany that the EBA provides preparatory work that helps specifying the content of the final legal national acts. In addition, the different instruments of the EBA are crucial for the interpretation of the PSD by fine-graining the European financial markets law.[3] The EBA's contributions are of pivotal functional prominence in terms of harmonization, standardization, and legal certainty.[4] However, according to the prevailing opinion in Germany and in other Member States, the EBA cannot enact legal instruments with immediate legal effect in domestic law.[5] At least from a German law perspective, legislative actions by the EBA with immediate effect would be constitutionally questionable, if not unconstitutional, and it is doubtful whether legislative power for European supervisory

[3] *J. Schemmel* (2019) Journal of Financial Regulation and Compliance, sub. 1.2.3.

[4] See in detail *E. Cervone*, SSRN 3209588, July 2, 2018, p. 5 et seqq. This is especially true for the interbank relationships that are governed by, inter alia, the SEPA Rulebooks.

[5] *E. Cervone*, SSRN 3209588, July 2, 2018, p. 6.

agencies would be in accordance with the European Treaties.[6] These doubts also concern the Regulatory Technical Standards on Strong Customer Authentication and common and secure communication (RTS)[7] that are devised by EBA. These are in fact binding law in all Member States after the Commission has endorsed them.[8]

From a German law perspective, it is also particularly remarkable that the EBA published an opinion on the elements of SCA on 21 June 2019,[9] in which EBA takes quasi-legislative actions while acknowledging the complexity of the payments markets across the EU and the challenges that arise from the changes that are introduced by the RTS. The EBA conceded that some actors in the payments chain, in particular those that are not payment service providers (PSPs), such as e-merchants, may not be ready to meet by 14 September 2019 all requirements set out by the RTS. In that regard, EBA took the exceptional step of empowering the national competent authorities (NCAs) to provide limited additional time for card-based payment online-transactions to allow card-issuing PSPs to migrate to authentication approaches that comply with SCA.[10]

---

[6] For further information on the European regulatory and supervisory structure of the financial markets, on the regulatory instruments, and on the dogmatics and legitimacy of EBA's instruments of action see *J. Schemmel*, Europäische Finanzmarktverwaltung – Dogmatik und Legitimation der Handlungsinstrumente von EBA, EIOPA und ESMA, 2018.

[7] Cf. https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2.

[8] For the legal basis see, inter alias, art 10 of the Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC.

[9] EBA, Opinion on the elements of strong customer authentication (SCA) under PSD2, EBA-Op-2019-06.

[10] The same applied to acquiring PSPs to migrate their merchants to solutions that support SCA.

In its additional opinion of 16 October 2019,[11] EBA stated that such supervisory flexibility of NCAs should end on 31 December 2020.

In response, the German Financial Supervisory Authority (BaFin) has made use of the leeway provided by the EBA. In its communications published on 21 August 2019 and 17 October 2019, BaFin allowed payment service providers domiciled in Germany to execute card-based payments online without Strong Customer Authentication (SCA).[12] Therefore, it is true that the EBA exerts some influence on the implementation of the PSD 2 into national law. However, the EBA's legislative impact is limited to particular aspects while direct exertion of influence is exceptional considering the aforementioned constitutional and European law concerns.

Having this said, the paper – according to my presentation at the conference – hereafter focuses solely on the role of the national legislator relating to the Directive's implementation into German law. It is not necessary to highlight the rules of national law in detail since the PSD 2 claims to be a full-harmonization directive. It is rather interesting to analyse the German legislator's choices made whenever the PSD 2 provided the Member States with a certain degree of regulatory freedom. Conceptually, there is only limited leeway for the legislator since the flexibility clauses contained in the PSD 2 only relate to regulatory niceties and details. Hence, I will turn to the areas of civil and supervisory law that are not explicitly regulated by the Directive. In reference to that, part two of the paper will explain some fundamentals of the German law on payment services, while part three to four will depict three particular decisions of the German rule maker that call for remarks.

---

[11] EBA, Opinion on the deadline for the migration to SCA for e-commerce card based payment transactions, EBA-Op-2019-11.

[12] See the press releases „PSD2: BaFin ermöglicht Erleichterungen bei Kundenauthentifizierung, 21.8.2019" and "PSD2 – BaFin setzt Frist zur Umstellung von Kartenzahlungen im Internet, 17.10.2019".

2. The basic structure of the Payment Services Law in Germany

First of all, it is necessary to sketch the basic structure of the Payment Services Law in Germany, as it is of quite unknown peculiarity in Europe. The implementation of the PSD 2 into national law was carried out by the so-called "Zahlungsdiensteumsetzungsgesetz" (ZUG).[13] In contrast to other Member States, the German legislator could not confine itself to simply reproduce the Directive's provisions since Germany does not have a dedicated Payment Services framework. The PSD 2, as the PSD 1 before, was rather implemented by the German ZUG segregated into two different legal frameworks: one part was transposed into the German Act on the Prudential Supervision of Payment Services, which is called "Zahlungsdiensteaufsichtsgesetz" (ZAG) and which is supposed to solely contain supervisory rules. The second part can be found in the German Civil Code (Bürgerliches Gesetzbuch; BGB) in sections 675c et seqq.

This separation can be explained by the dogmatic notion in Germany that legal norms are resting on different pillars. Supervisory law is considered public law; all other rules that are not criminal law provisions are civil law provisions. Therefore, one main objective of the German legislator was to identify the supervisory and civil law provisions within the PSD 2. Then he had to dissolve the different statutes from each other and implement them into the appropriate legal domestic regime. Such a rather unusual transposition of a Directive can provide frictions, but it also has a very tangible legal significance. An example might illustrate the *raison d'être* for the transposition of the PSD into German law:

[13] See Bundesgesetzeblatt (BGBl.) 2017, Part I No 48, p. 2446. For reference and for the draft bill see www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/18_Legislaturperiode/2017-07-21-Umsetzung-Zweite-Zahlungsdienstrichtlinie/0-Gesetz.html.

Assume the payer became the victim of a phishing attack and that he revealed with gross negligence the personalized security features of its online banking to a third person. As a result, ten unauthorized payment transactions were initiated each in the amount of 201 EUR (overall 2010 EUR). According to the Payment Services Law[14], the payer is obliged to provide compensation to his payment service provider with regard to the entire damage caused as a result of the unauthorized payment transaction since he grossly negligently violated his obligation to take all reasonable precautions to protect the personalized security features against unauthorized access.[15] Now further assume that the payment services provider's algorithms detected that all unauthorized transactions were initiated within 30 seconds out of India. It would have been easy by means of the algorithmic system to prevent the transactions based on the transaction's information and to ask the payer whether he had actually made the payments. However, the payment services provider ignored the indications for misconduct he had obtained from the transaction monitoring. Since the German legislator transposed the liability rules into the German Civil Code[16], it is clear that the payment service provider is entitled to a civil-law claim for damages in case of abusive use of a payment instrument caused by the payer's misconduct. Consequently, the "mirror image rule" to the claim for damages, also called the rules on joint-responsibility (*Mitverantwortung*)[17], apply to the detriment of the payment service provider. According to this rule, first, the plaintiff – here the payment service provider – cannot recover damages that he ought to have avoided by himself, and second, any contributory fault or negligence (*Mitverschulden*) of the affected plaintiff may be taken into account and the amount that can be claimed for damages is to be reduced accordingly. In our case, it can be argued that the affected payment service provider could have spotted the irregularities in the transaction and he ought

[14] See in Germany section 675v (2) BGB; see also art 74 (2) PSD 2.

[15] See section 675l BGB; art 69 (2) PSD 2.

[16] See section 675v BGB.

[17] See section 254 BGB; for explanations cf. *B. Markesinis/H. Unberath/A. Johnston*, The German Law of Contract, 2006, p. 475 et seq.

to have prevented the transaction from being executed. Hence, contributory negligence (*Mitverschulden*) of the affected payment service provider is to be taken into account and the amount that can be claimed for damages is to be reduced.[18] Depending on the individual case, it is even possible to argue that the payment service provider's responsibility is so predominant that the payer does not have to pay any compensation at all. However, the reasoning behind the applicability of the rules on contributory negligence is important: The aim is to ensure that the Payment Services Law does not create false incentives on the part of the payment services providers. That would be the case though if their behaviour were totally disregarded in the assessment of the claim for damages.

If the civil law claim for damages of the PSD had not been implemented by the German legislator into the Civil Code, it would not have been clear whether the rules on contributory fault or negligence (*Mitverschulden*) apply. Other countries that compiled a dedicated Payment Services Act have reported, the applicability of the rules on contributory fault is highly controversial in the respective jurisdictions. This is not the case in Germany, since the realm of the Directive's implementation automatically invokes the general liability provisions of the German Civil Code. These provisions also comprise the rules on joint-responsibility (*Mitverantwortung*). This approach to the transposition of the PSD complies with European Law since the PSD 1 and the PSD 2 do not provide any provisions on the *topos* of joint-responsibility and do not turn against these rules, either.

3. The so-called Anscheinsbeweis-rule in Germany

In comparison to the PSD 1, the revised PSD 2 contains an amendment of art 72 on evidence on authentication and execution of payment transactions. Art 72 para 2 sentence 2 PSD 2, which was not part of the PSD 1, now reads:

[18] For the applicability of the rule on contributory fault in payment service law, see BGH, 24.4.2012 – XI ZR 96/11, Neue Juristische Wochenschrift (NJW), 2012, 2422, recital 29 et seqq.; *S. Omlor*, in: Staudinger, BGB, 2020, § 675v, Rn. 30 et seq.

> "The payment service provider, including, where appropriate, the payment initiation service provider, shall provide supporting evidence to prove fraud or gross negligence on part of the payment service user."

At first glance, the textual expansion of the rule on evidence is incomprehensible, as sentence 1 of art 72 para 2 PSD 2 states:

> "Where a payment service user denies having authorized an executed payment transaction, the use of a payment instrument recorded by the payment service provider (...) shall in itself not necessarily be sufficient to prove either that the payment transaction was authorized by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfill one or more of his obligations."

That means that both sentences essentially state the same – at least as far as they refer to potential misconduct of the payer.

Yet, in order to understand the second sentence, one needs to consider the study on the impact of the PSD 1.[19] There it is said that national law based on prima facie evidence in cases of unauthorized transactions has not changed after implementation of the PSD 1, although the first sentence of art 72 para 2 did already existed in the PSD 1. In essence, the study criticizes that the regulatory objectives were missed. The study observes that "German consumers must still bear the entire loss" and that similar problems have been reported by associations from Denmark and Sweden. This means that, with its new sentence 2, the PSD 2 tried to avoid any automatism of evidence to the detriment of the customer – believing that such an automatism was, inter alia, in Germany in place. The background to this assumption is a German rule on evidence known commonly as

[19] Study on the impact of Directive 2007/64/EC on payment services in the internal market and on the application of Regulation (EC) No 924/2009 on cross-border payments in the Community, Contract MARKT/2011/120/H3/ST/OP – Final report, p. 239 et seqq.

"Anscheinsbeweis" (*prima facie evidence*).[20] The Anscheinsbeweis was developed by the German Federal Supreme Court (BGH).[21] Courts apply the Anscheinsbeweis to discharge payment service provider of the burden to present evidence of pertinent circumstances that inherently cannot be detected since they lie within the inaccessible customer's sphere. For example: If a debit card was used along with the PIN at an ATM in Bergamo (Italy), then the circumstances *prima facie* imply that it was the customer himself who made the withdrawal. It is then up to the customer to prove that he wasn't able to do so since he was giving lectures in Mannheim (Germany) that very same moment.

The *prima-facie*-rule may not be confused with an irrebuttable presumption of proof (Beweisvermutung) since it merely relieves the plaintiff of its burden of proof. Thus, the Anscheinsbeweis is just a facilitation of proof (Beweiserleichterung).[22] The customer does not need to fully rebut the *prima-facie*-rule by providing counterevidence. Instead, the customer needs to contest the evidence-rule based assumption by submitting sensible arguments and facts in a court hearing. Hence, the *prima-facie*-rule simply tries to take into account that facts stem from different spheres of influence (Verantwortungsbereiche) and that these facts cannot be reviewed by both parties nor does one party have the means to obtain knowledge about these facts within the area of control of the other party. Hence, to distribute burdens of proof appropriately, both the payer and the payment service provider are in each case responsible for facts within their own sphere. With the help of

[20] The rule generally does apply to all kinds of payment methods (cf. Online Banking, cash withdrawal at ATMs, debit card payments at the point of sale, etc.).

[21] See BGH, 26.1.2016, XI ZR 91/14, ECLI:DE:BGH:2016:260116UXIZR91.14.0; first developed in BGH, 5.10.2004, XI ZR 210/03, Neue Juristische Wochenschrift (NJW), 2004, p. 3623 (in this case, a PIN-based ec-card was exposed and then misused).

[22] *D. Linardatos*, Neue Juristische Wochenschrift (NJW), 2017, 2145 (2146) with further references.

the *prima-facie*-rule, the courts try to impose the onus on the party who is in control of the circumstances that need to be proven and is hence in control of the evidence itself.

Now, regarding the aforementioned meaning of the *prima-facie*-rule, did the German legislator decide to exclude the Anscheinsbeweis in order to comply with the revised text of the PSD 2? There is no clear-cut answer to this question, since the legislator failed to express its opinion on this issue, leaving it to scholars and practitioners to determine the exact significance of the revised evidence rule in the PSD 2. However, according to the prevailing academic opinions, the *prima-facie-rule* does apply in payment services in Germany despite the revision of the PSD 2.[23] It is argued by different scholars that the national legislator was not obliged to rule out the Anscheinsbeweis since the PSD 2 just reiterated its position that Member States have to avoid an evidence rule that always applies in favour of the payment service provider and that, in fact, cannot be disproven by the customer. Hence, it can be reasoned that there is no need to change the national procedural law if there is no irrefutable rule.

Indeed, such irrefutable rule to the detriment of the customer – as shown above – did never exist in German law. The Anscheinsbeweis is only intended to prevent an exorbitant onus of proof to the one-sided drawback of the payment services provider. This implies that, insofar as the *prima-facie*-rule is concerned, the impact study[24] is faulty reporting on the German jurisdiction. According to the German Federal Supreme Court (BGH), the *prima-facie*-rule does only apply if[25],

---

[23] *D. Linardatos*, Neue Juristische Wochenschrift (NJW), 2017, 2145 et seqq.; agreeing *S. Omlor*, Juristische Schulung (JuS), 2019, 289 (293); *K. Zahrte*, Neue Juristische Wochenschrift (NJW), 2018, 337 (340 et seq.); *O. Böger*, in V. Baas/P. Buck-Heeb/S. Werner (Ed.), Anlegerschutzgesetze, 2018, § 675w recital 30.

[24] Cf. *supra* footnote 18.

[25] See BGH, 26.1.2016, XI ZR 91/14, ECLI:DE:BGH:2016:260116UXIZR91.14.0, recital 27 et seqq.; prerequisites summarized in *D. Linardatos*, in Karsten Schmidt (Full Ed.), Münchener Kommentar zum HGB, Band 6: Bankvertragsrecht, 4th Edition 2019, K. Online-Banking, recital 250 and 254.

- first: the payment service provider proved that the payment transaction was authenticated, accurately recorded, entered into the accounts and not affected by a technical breakdown or some other deficiency of the service provided by the payment service provider – which means that the payment service provider must have met the requirements of section 675w BGB;
- second: a security system has been used that is virtually impossible to tackle and the interference of an unauthorized third party with the communication channel between payer and payment service provider is practically excluded;
- third: a dynamic TAN was used for the transaction and the payment service user was given the opportunity of reviewing the payment order before the transaction was released, which means that the requirements of the SCA must have been met.

One clear-cut example of a system that is not sufficiently secure is the now out-of-use paper TAN-list. Another example of a system that does not fulfil the Court's criteria to apply the *prima-facie*-rule is the mobile TAN-system. According to the German Federal Supreme Court, the fact that several reports of successful hack attempts on the mobile-TAN-system are known is reason enough to exclude the *prima-facie*-rule. This assessment is of particular relevance since the mobile TAN-system does fulfil the requirements on SCA. Hence, it is fair to conclude that the requirements defined by the BGH in order to apply the *prima-facie*-rule are even stricter than the requirements set out in the Regulation on Strong Customer Authentication. Thus, the German legislator acted rightfully when he decided not to exclude the *prima-facie*-rule. In fact, legal scholars in Germany argue that art 72 para 2 sentence 2 of the PSD 2 can be simply ignored since the provision does not add noteworthy obligations.[26]

[26] Cf. proofs in footnote 22; dissent *Keßler*, in Ebenroth/Boujong/Joost/Strohn (Ed.), Handelsgesetzbuch, 4th Edition 2020, Section 675w recital 11 with footnote 27.

4. The supervisory regulation of the Third Party Service Provider (TPP) and its effects on Civil Law

The PSD 2 introduced a regime to foster sharing of payment account data among banks and payment services provider. One goal was to create a user customer experience, which is better tailored to daily needs of a digitized society. It is argued that by requiring large banking incumbents to share data via an open application programming interface (API), Third Party Service Providers (TPP) are able to provide various services tailored to the customers' individual profiles.[27]

One interesting decision of the German legislator that is noteworthy relates to these TPP. As mentioned before, the PSD 2 was implemented into two different legal frameworks. Art 66 and 67 PSD 2 regarding the rules on access to a payment account and payment account information in the case of the use of a payment initiation service or the use of account information services were mainly transposed into the ZAG.[28] Hence, by its regulatory nature, the right of access is supervisory law. Also, art 68 PSD 2, which regulates the limits of the use of the payment instrument and the access to payment accounts by payment service providers, was transposed into the ZAG.[29] By implementing these rules into the regulatory framework of the ZAG, the German legislator tried to clarify that the provisions serve public interests only. The provisions do not create a subjective claim of the TPP against the BaFin. Therefore, these TPP cannot claim damages from the BaFin for non-performance if the account servicing service provider refused to grant to the third-party service access to the payer's account without reason. Hence, the BaFin does intervene only in the interest of the public, but not to enforce the individual interests of the TPP.

---

[27] *B. Regnard-Weinrabe/J. Finlayson-Brown*, in J. Madir (Ed.), Fintech. Law and regulation, 2019, Chapter 2, recital 2.48 et seqq.

[28] There in the sections 48 et seqq.

[29] See section 52.

Instead, the third parties have to claim damages in civil proceedings against banking incumbents.

It is also noteworthy that according to the prevailing opinion in Germany, the transposition of the arts 66 et seqq. into the ZAG is partly misplaced. The provisions that are regulating the access to payment accounts contain due diligence obligations and procedural obligations. For instance, sec 48 of the ZAG states, inter alia:

> "The payment service provider running the payment account shall be obliged to communicate with the payment initiation service provider securely."

It is quite clear that such an obligation must also have implications on the Civil Law regime. A customer cannot be liable for the loss occurred due to unauthorized payment transactions, if the reason for that loss is a breach of supervisory duties by the payment services provider. Therefore, it is fair to say – in a generalized sense – that in Germany there are supervisory obligations in place that can actually affect civil law claims.[30] It is possible for a claimant to invoke administrative law as a benchmark against which the defendants conduct is to be assessed.[31] And it is quite easy to justify the validity of this opinion: European Directives are binding as to the economic and applicatory[32] objects whilst the dogmatic approaches of the Member State's legal regime are irrelevant. To strictly differentiate between Supervisory Law and Civil Law is widely unknown in European legal systems. This distinction is even

---

[30] *S. Omlor*, Wertpapier-Mitteilungen (WM), 2018, p. 57 et seqq.; *D. Linardatos*, in Karsten Schmidt (Full Ed.), Münchener Kommentar zum HGB, Band 6: Bankvertragsrecht, 4th Edition 2019, K. Online-Banking, recital 157 et seqq.

[31] In financial markets, this approach applies in different jurisdictions as it is outlined by European Expert Group on Liability and New Technologies, Report on Liability for Artificial Intelligence and other emerging digital technologies, 2019, p. 18.

[32] That means it does not matter what the effect is from a dogmatic point of view.

unknown to European Law itself. Hence, Member States cannot limit the effects of a Directive with reference to national dogmatic peculiarities. The transposition of the Directive is not in the Member State's discretion as far as the actual implications of harmonizing regulations are concerned. It is one main feature of the "*effet utile*"-principle that supervisory regulations need to be considered in civil proceedings, if otherwise inconsistent results cannot be prevented.[33]

5. Requirements on Strong Customer Authentication (SCA)

In the following I will address the decision of the German legislator about the requirements for Strong Customer Authentication (SCA). The relevant provisions of the PSD 2 are solely implemented into the Payment Services Supervision Act. This decision seems to be slightly off. According to the PSD 2,[34] the payer's civil liability for any financial losses due to unauthorized payment transactions is excluded, if the payer's payment service provider does not require SCA, unless the payer has acted fraudulently. The legislative decision to implement the provisions on SCA into the supervisory regime led to the discussion whether the conditions of the civil liability exemption and the supervisory requirements on SCA are the same. Some German scholars are inclined to say that the civil law exemption rule is sterner than the supervisory requirements. While supervisory law requires SCA only for electronic payment transactions, Civil Law would require SCA for each payment transaction (e.g. for credit card transactions with payment vouchers).

---

[33] For groundwork on the relationship between supervisory requirements and civil liability norms in payment services cf. *S. Omlor*, Wertpapier-Mitteilungen (WM), 2018, 57 et seqq.; *S. Omlor*, Zeitschrift für Bank- und Kapitalmarktrecht (BKR) 2019, 105, 113; *D. Linardatos*, in Karsten Schmidt (Full Ed.), Münchener Kommentar zum HGB, Band 6: Bankvertragsrecht, 4th Edition 2019, K. Online-Banking, recital 157 et seqq.

[34] See art 74 para 2.

Here again we have Janus-faced provisions that were implemented misleadingly by the German legislator because German lawyers are generally hesitant to discard the segmentation of the law in legal pillars. Basically, the German legislator again just wanted to clarify that the provisions on the requirements on SCA do not provide a claim for damages of the payer against the German Supervisor for non-performance. However, a payment service provider cannot be the addressee of contradicting obligations on the same issue. Such an interpretation of the law would unnecessarily hinder the realization of a harmonized European Single Market. Hence, the supervisory requirements and the civil requirements on SCA are essentially the same. The Supervisory Law is here again influencing the civil law obligations and liability rules.

6. The unclear relationship between GDPR and PSD 2

Until now, I outlined some decisions that were made by the German legislator. In the last part of this paper, I want to mention one problem the national legislator did not solve. As in other countries, there is legal uncertainty in Germany about the interrelation between the General Data Protection Regulation (GDPR)[35] and the PSD 2. On the one hand, the PSD 2 generally aims at driving innovation in payment services by making it easier to share data.[36] On the other hand, the regulatory aims of the GDPR are, inter alia, data minimization and earmarking, since under the GDPR personal data shall only be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those

[35] 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.

[36] *B. Regnard-Weinrabe/J. Finlayson-Brown*, in J. Madir (Ed.), Fintech. Law and regulation, 2019, Chapter 2, recital 2.69.

purposes".[37] Therefore, payment institutes face the problem of having to deal with conflicting goals between PSD 2 and GDPR. I want to focus on one particular issue: According to art 67 PSD 2, the account information service is not allowed to

> "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."

What does this mean? Is it possible to obtain the user's explicit consent to use the data for purposes other than performing the account information under the rules of the GDPR or does the PSD 2 provide the more specific rules that supersede the GDPR provisions? The relationship between PSD 2 and GDPR is a highly critical issue as an entire industry depends on the data it obtains through account information services (e.g., for marketing purposes). If the PSD 2 is deemed to overrule the consensus principle of the GDPR, account information services would no longer be able to sell data *although* they would be acting within the customer's approval. But why shouldn't it be possible to obtain the customer's consent under the GDPR's principles? After all, art 6 para 1 lit. a GDPR states that data processing shall be lawful if and to the extent that the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

Solely the legislator of the European Union can define conclusively on the interplay between GDPR and PSD 2. The European lawmaker needs to be aware – above all in data protection and data law – that it is not appropriate to establish parallel rules that ignore any possible interrelations. The legislator needs to rectify the unclear relationship between GDPR and PSD 2 on a union-wide basis. The e-commerce and the e-payment services sector are in dire need of clarification through harmonized legislation since

[37] See art 5 (1) (b) GDPR.

they are depending on the harvesting of data. In the meantime, the Member States will have to try to interpret the various legal complexes in a coherent way. The expression of an opinion by the German legislator within the implementation process of the PSD 2 would have been beneficial, but it refrained from doing so in order to avoid the risk of legislation contradicting European law. Hence, it is up to legal scholars to submit helpful and coherent suggestions.

In my opinion, it is convincing to suppose that data processing within the principles of the GDPR should be considered as valid also under the rules of the PSD 2. One of the main objectives of the PSD 2 is to support and facilitate innovative payment instrument services. This objective will be missed if the PSD 2 rules that are related to data law issues are interpreted in an unduly strict manner. The regulatory core aim of the PSD 2 – apart from the promotion of innovation – is to increase consumer protection. That includes a general enhancement of the levels of security for electronic payment services. These aims are not impaired at all if the payment service provider obtains the data subject's consent in compliance with the rules of the GDPR. The regulatory purposes of the PSD 2 and the GDPR overlap on the margins, but they differ with regard to the regulatory nucleus. The main objective of the GDPR is enhancing data protection while the main objective of the PSD 2 is to increase consumer protection in payment services. PSD 2 and GDPR should, therefore, be treated as complementing legal frameworks. As far as the process of data collection by a payment services provider is in line with the rules and the fundamental principles of the GDPR, the PSD 2 rules should step back. Thus, in cases of doubt, I plead for a primacy of the GDPR – not least because the GDPR is the more recent and is, regarding data protection issues, the more comprehensive legal act. This interpretation ensures that the development of use-friendly and innovative payment systems is not jeopardized while the obligations of the PSD 2 assures that electronic payment services are carried out in a secure manner and by technological means that guarantee the safe authentication of the user and that cut the risk of fraud.

7. Overall impacts of the PSD 2 in Germany

In summary, it is fair to say that the PSD 2, on the one hand, has led to quite peculiar legal uncertainties in Germany, which are caused by dogmatic thinking in categories. The regulatory requirements became increasingly complex. On the other hand, the implementation of the PSD 2 in two different parts helps to establish a balanced statutory system and it provides legal certainty that is missing in other Member States.

Furthermore, the Directive's overall economic effects in Germany are positive. The liberation of the Payment Services Law by integrating TPP fostered the competition between incumbent banks and innovative newcomers and facilitated the growth of new mobile payment technologies. However, payment and data protection laws still need to be aligned. It is fair to say that a Third Payment Services Directive is inevitable and that such an act mainly needs to address data protection issues since the reliability of payment services is already well advanced thanks to the PSD 1 and PSD 2.

Bibliography

O. Böger, in V. Baas/P. Buck-Heeb/S. Werner (Ed.), Anlegerschutzgesetze, 2018.

E. Cervone, The European Banking Authority in Light of the CJEU Jurisprudence: The Case of Innovative Payment Services, SSRN 3209588, July 2, 2018.

O. Keßler, in Ebenroth/Boujong/Joost/Strohn (Ed.), Handelsgesetzbuch, 4th Edition 2020.

D. Linardatos, Von Anscheinsbeweisen im Zahlungsdiensterecht und fehlgeleiteten Gesetzgebern, Neue Juristische Wochenschrift (NJW), 2017, pp. 2145–2150.

D. Linardatos, in Karsten Schmidt (Full Ed.), Münchener Kommentar zum HGB, Band 6: Bankvertragsrecht, 4th Edition 2019, K. Online-Banking.

B. Markesinis/H. Unberath/A. Johnston, The German Law of Contract, 2006.

S. Omlor, in von Staudinger (Ed.), Kommentar zum Bürgerlichen Gesetzbuch: Staudinger BGB - Buch 2: Recht der Schuldverhältnisse: §§ 675c–676c (Zahlungsdienstrecht), 2020.

S. Omlor, Digitaler Zahlungsverkehr, Juristische Schulung (JuS), 2019, pp. 289–294.

S. Omlor, Zahlungsdiensteaufsichtsrecht im zivilrechtlichen Pflichtengefüge, Wertpapier-Mitteilungen (WM), 2018, p. 57.

B. Regnard-Weinrabe/J. Finlayson-Brown, in J. Madir (Ed.), Fintech. Law and regulation, 2019.

J. Schemmel, Regulating European financial markets between crisis and Brexit, Journal of Financial Regulation and Compliance (2019), pp. 503–514.

J. Schemmel, Europäische Finanzmarktverwaltung – Dogmatik und Legitimation der Handlungsinstrumente von EBA, EIOPA und ESMA, 2018.

K. Zahrte, Neuerungen im Zahlungsdiensterecht, Neue Juristische Wochenschrift (NJW), 2018, pp. 337–341.

Maria Raquel Guimarães[1]
(University of Porto)

THE TRANSPOSITION OF PSD2: DECREE-LAW 91/2018 OF 12 NOVEMBER, THE PORTUGUESE EXPERIENCE AND WHAT MAY (OR MAY NOT) CHANGE

1. Decree-Law 91/2018 of 12 November 2018: scope and subject matter

The second Directive on Payment Services (DSP 2) — Directive (EU) 2015/2366 — was transposed to Portuguese law by Decree-Law 91/2018 of 12 November, introducing the *New legal framework for payment and Electronic money services*, nine months after the deadline established by the European Union for national compliance with the Directive and after the first Directive on Payment Services (PSD 1) was repealed, on 13 January 2018.[2]

The first point to be made regarding the Portuguese Act is that it contains 162 articles, over 50 more than PSD2. The reason for the great increase in the number of articles is the fact that in 2012 Portugal chose not to adopt a new *ad hoc* act to implement Directive

[1] Professor of Civil Law and Contract Law, Faculty of Law, University of Porto, Portugal. Researcher at CIJE — Centre for Legal and Economic Research/Centro de Investigação Jurídico-Económica (University of Porto, Portugal)

[2] See articles 114 and 115 of 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) 1093/2010, and repealing Directive 2007/64/EC, *OJ* L 337, 23.12.2015, pp. 35-127.

2009/110/EC on Electronic money.[3] Instead, the Electronic money Directive was transposed through Decree-Law 242/2012 of 7 November, amending the act on payment services that appeared in 2009 — Decree-Law 317/2009 of 30 October —, shortly after this new Directive had been published. This means that since 2012, the Portuguese first act on payment services has simultaneously been governing payment services, as defined in PSD 1, and also Electronic money services, complying with the Electronic money Directive.

Again, in 2018, faced with the new task of incorporating the new payment services directive to Portuguese law, it was decided by the legislator that the two-in-one model of 2012 should be kept, and section IV of the new law was dedicated to Electronic money.

In 2012, this option was already based on three main arguments: first of all, the complementary relationship between E-money and payment transactions was stressed, and Electronic money was also considered to have a payment function. Secondly, the rule makers pointed out that the typology of Electronic money issuers is virtually identical to that of payment service providers. In addition, Electronic money institutions are entitled to provide any of the payment services included in PSD, which places their activity within the scope of both Directives. Finally, regardless of certain specificities, the authorization and supervision regime for Electronic money institutions is largely based on the regime for payment institutions.[4]

Based on these criteria, Portugal has had a single act on payment services *and* Electronic money since 2012, a *status quo* that the transposition of PSD2 has not changed.

---

[3] 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, *OJ* L 267, 10.10.2009, pp. 7-17.

[4] See the preliminary text that introduces Decree-Law 242/2012 of 7 November.

The Portuguese payments act — Decree-Law 91/2018 — also includes the necessary rules to comply with the following regulations:[5]

a) Regulation (EC) 924/2009 of the European Parliament and of the Council of 16 September 2009 on cross-border payments in the Community and repealing Regulation (EC) 2560/2001;[6]
b) Regulation (EU) 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) 924/2009;[7] and
c) Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions.[8]

At the same time, complying with the new PSD2 rules, the Portuguese Act has widened the scope of application of the former legal framework for payment and Electronic money services in order to include new types of "open banking" services, in particular payment initiation services and account information services.[9] These services, mostly payment initiation services, have proved

[5] See articles 146-149, Title VI.

[6] *OJ* L 266, 9.10.2009, pp. 11-18.

[7] *OJ* L 94, 30.3.2012, pp. 22-37.

[8] *OJ* L 123, 19.5.2015, pp. 1-15.

[9] See PSD2**,** recitals 27-29 and article 4 (15)(16), and Decree-Law 91/2018, article 2 (tt)(uu). The inclusion and the regulation of the activities of these two new players on the payments' market is considered by several authors to be one of the key changes in PSD2. See Mª N. Pacheco Jiménez, "La nueva directiva 2015/2366 de servicios de pago en el mercado interior", *in Revista CESCO de Derecho de Consumo*, no 16/2016, p. 141, <https://revista.uclm.es/index.php/cesco> (25.01.2020); M. Donnelly, "Payments in the digital market: Evaluating the contribution of Payment Services Directive II", *in Computer Law & Security Review*, no 32, 2016, pp. 829-832; R. Steennot, "Reduced payer's liability for unauthorized payment transactions under second Payment

to be an appealing alternative to "traditional" online payments based on cards and allow consumers to pay for goods or services in e-commerce transactions without disclosing their banking data to the seller. According to PSD2, payment initiation services provide a "software bridge" between the seller website and a home banking platform.[10] A payment order is initiated "at the request of the payment service user with respect to a payment account held at another payment service provider",[11] encouraging the payee to deliver the goods or services without delay. Considered by the European institutions as a "low-cost solution" for both parties on an Internet payment transaction,[12] one of the main purposes of the new directive has been the expansion of its scope in order to cover these types of Internet payment services under its rules. In particular the rules on the allocation of liability for unauthorised transactions were extended to the new intermediary partners, to clear the doubts that emerged from the exclusions made by the first directive and consequently by national laws.[13]

Services Directive (PSD2)", *in Computer Law & Security Review*, no 34, 2018, pp. 954-956; and F. Mendes Correia, "Uma revolução permanente? A DSP 2 e o novo Direito dos Serviços de Pagamento", *in III Congresso de Direito Bancário*, [L. M. Pestana de Vasconcelos (coord.)], Coimbra, Livraria Almedina, 2018, pp. 388, 394-395. For further developments on the difficult balance between the activity of these two new players and consumers' security and privacy, especially the problems that can result from the data processing of accounts on a large scale, see P.T.J. Wolters / B.P.F. Jacobs, "The security of access to accounts under PSD2", *in Computer Law & Security Review*, no 35, 2019, pp. 29-41.

[10] PSD2, recital 27. M. Donnelly, "Payments in the digital market...", p. 830, characterize this service also as an "overlay service".

[11] See PSD2, article 4 (15).

[12] PSD2, recital 29.

[13] See PSD2, article 73 (2), and Decree-Law 91/2018, article 114 (5-9).

2. "Filling the gaps" on PSD2

Portugal has taken advantage of some of the few possibilities the European Union has left to each Member State on PSD2 to adjust or adapt its provisions to national realities, disregarding other options and, in those cases, just adhering to the basic model offered by the directive.

2.1. Exclusions

Focusing not on all the "gaps" Member States could fill in, but on some selected topics that we consider most relevant, and still looking at the scope — the subjective scope — of the Portuguese Act *versus* the directive, it should be mentioned that Portugal did not use the possibility provided by article 2 (5) of PSD2 to exempt the institutions referred to in point (19) of article 2 (5) of Directive 2013/36/EU[14] from the application of all or part of the provisions of PSD2: in Portugal, targets were *Caixas Económicas* existing on 1 January 1986, and they were not excluded from the Portuguese Act.

Nevertheless, the Portuguese Act has used the possibility to allow *Banco de Portugal* to exempt natural or legal persons providing payment services [as referred to in points (1) to (6) of Annex I] from the application of all or part of the procedure and conditions set out in Sections 1, 2 and 3 — with the exception of articles 14, 15, 22, 24, 25 and 26 — as far as these persons comply with the conditions of the Directive.[15] And these conditions are, firstly, that the monthly average of the preceding 12 months' total value of payment transactions executed by the person concerned, including any agent for which it assumes full responsibility, does not exceed

[14] 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, *OJ* L 176, 27.6.2013, pp. 338-436.

[15] See PSD2, article 32, and Decree-Law 91/2018, article 37.

3 million euros; and, secondly, that none of the natural persons responsible for the management or operation of the business has been convicted of offences relating to money laundering or financing of terrorist activities or any financial crime. And *Portaria* 239/2019 of 30 July has added that legal persons exempt from the proceedings and conditions set out in the referred articles must hold a share capital of at least 50,000 euros.[16]

2.2. Microenterprises and consumers

With regard to microenterprises, Portugal has maintained the option made in 2009 to apply the rules on transparency of conditions and information requirements for payment services to microenterprises — as defined in Commission Recommendation 2003/361/EC —[17] in the same way as to consumers.[18]

However, this equation is excluded from microenterprises that agree with their payment service provider that there is no right to reimbursement for unauthorized debit transactions, thus enabling them to access the SEPA B2B direct debit model.[19]

---

[16] Article 3 (2), *Portaria* 239/2019 of 30 July.

[17] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, article 2 (3): "Within the SME category, a microenterprise is defined as an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million".

[18] See PSD2, article 38 (2), and Decree-Law 91/2018, article 76 (2).

[19] Decree-Law 91/2018, Preamble paragraph 18, and article 117 (7): microenterprises are authorised by national law to opt out from the refund right in order to access the SEPA B2B direct debit model. Nevertheless, on its FAQs on direct debits, *Banco the Portugal* displays on its portal a different solution: "In accordance with the legislation in force, reimbursement is an inalienable right of debtors (consumers and microenterprises) as regards direct debit transactions. As such, microenterprises operating in Portugal cannot, as debtor entities, participate in the SEPA B2B direct debit scheme, but only in the SEPA CORE direct debit scheme (given that the first does not envisage the right to reimbursement)." *In* <https://www.bportugal.pt/en/perguntas-frequentes/260/print> (25.01.2020).

Rules on rights and obligations in relation to the provision and use of payment services — articles 62 ff. of PSD2 — are also applicable to microenterprises in the same way as to consumers.[20]

Finally, concerning the termination of the framework contract, the Portuguese law has used the prerogative to provide for more favourable provisions for payment service users and has disposed that this termination shall always be free of charge for consumers as well as for microenterprises.[21]

2.3. Other provisions

As for low-value payment instruments, Electronic money and prepaid payment instruments, Portugal has neither reduced nor increased the amounts referred to in articles 42 and 63 of PSD2 for the derogation, for national payment transactions, from information requirements and from rights and obligations in relation to the provision and use of payment services. Limits have been maintained regarding payment instruments which concern only individual payment transactions that do not exceed 30 euros or that either have a spending limit of 150 euros or store funds that do not exceed 150 euros at any time.[22]

At the same time according to article 96 (3) of the Portuguese act the framework contract must include a condition saying that the payment service user may require payment service providers to deliver information on paper or on another durable medium at least once a month, free of charge. This was a possibility opened up by PSD2 in order to take into account different national practices concerning information provided to the user.[23]

---

[20] See PSD2, article 61 (3), and Decree-Law 91/2018, article 100 (1).

[21] See PSD2, article 55 (6), and Decree-Law 91/20, article 94 (2).

[22] See PSD2, articles 42 (1) (2), 63 (1) (2), and Decree-Law 91/2018, articles 81 (1), 102 (1).

[23] See PSD2, article 58 (3).

On the subject of applicable charges, PSD2 states that Member States may prohibit or limit the right of the payee to request charges, taking into account the need to encourage competition and promote the use of efficient payment instruments.[24] With this base, Portugal has ruled that the payee cannot request charges where there is a legal provision limiting this right to encourage competition or to promote the use of effective payment instruments, leaving the matter for rule makers to decide where competition must be encourage or effective payment instruments are needed.[25]

Lastly, as far as national payment transactions are concerned, Portugal has disposed that for transactions made between accounts with the same payment service provider, and in the absence of any stipulation to the contrary, funds shall be credited to the payee's account on the same day, with the value date and the availability of funds date being at the time of credit, taking into account the efficiency of these transactions.[26]

3. Sequence. User's liability for unauthorised payment transactions

On the user's liability for unauthorised payment transactions, PSD2 rules that the user shall bear all of the losses relating to any unauthorised payment transactions if they were incurred by the user acting *fraudulently* or failing to fulfil one or more of the obligations in relation to payment instruments and personalised security credentials *with intent* or *gross negligence*.[27] Nevertheless,

[24] See PSD2, article 62 (5). For further developments on this applicable charges, see M. R. Guimarães, "Los medios de pago en el derecho europeo y en los instrumentos europeos de armonización del derecho privado", *in Banca, Borsa, Titoli di Credito*, vol. 70, no 4, Milano, Giuffrè Editore, 2017, pp. 564-566.

[25] See Decree-Law 91/2018, article 101 (5c).

[26] See PSD2, article 86, and Decree-Law 91/2018, article 127.

[27] See PSD2, article 74 (1) *in fine*. Literally, article 74 refers to the "payer's liability" and not the "user's liability", as already was the case in PSD 1. However, according to PSD2 article 4 (8), the "payer" is "a natural or legal person who holds a payment

PSD2 allows Member States discretion to reduce the user's liability where he/she has acted merely with gross negligence.[28]

According to Portuguese law, where the user has neither acted fraudulently nor intentionally failed to fulfil these obligations, but only acted with *gross negligence*, his or her liability is reduced to the credit limit of the respective account or of the payment instrument, or to the limit of his or her available balance.[29] This solution had already been adopted in 2009 and the new legal framework for payment services has chosen to maintain the same rule.

Clearly, Portuguese law has not taken into account the nature of the personalised security credentials and the specific circumstances under which the payment instrument was lost, stolen or misappropriated, as referred to in PSD2, but established a ceiling for the users' liability, which may or may not be the equivalent of all of the losses suffered by them, depending, namely, on the overdraft permitted by the provider. The particular circumstances that lead to an unauthorised transaction are then taken into account by the court, which measures the importance of the user's negligent conduct and its influence on the damages.

---

account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order". Whenever an unauthorized payment occurs, the bank customer *does not allow* a payment order *nor does he/she give a payment order* and that is precisely why the payment is unauthorized... The person who gives the payment order is a third person, probably in the context of a fraudulent scheme. And it is not this third person that is the subject of the provisions of article 74, nor is he/she the person entitled to the refund of article 73. The Portuguese Act also refers to the "payer" and not the "user" in this context. Regarding this inattention of the European law makers, see M. R. Guimarães, "The debit and credit card framework contract and its influence on European legislative initiatives", *in InDret Comparado*, *Revista para el Análisis del Derecho*, no 2, 2012, pp. 13-15, <http://www.indret.com/pdf/892_en.pdf> (25.01.2020). On the concept of "unauthorized payment", see R. Steennot, "Reduced payer's liability for unauthorized payment transactions under second Payment Services Directive (PSD2)", pp. 955-956.

[28] M. Donnelly, "Payments in the digital market...", p. 835, notes that this provision for Member States discretion contradicts the great aim of full harmonization assumed by PSD2.

[29] See Decree-Law 91/2018, article 115 (4).

4. Case Law: What may (or may not) change

Since PSD2 was implemented in Portugal on 12 November 2018 and came into force on the next day it is too early to find any case law based on the new act. Nevertheless, the Portuguese experience with regard to the 2009 Act may be significant and we may speculate how the new rules will change the patterns set by the previous courts decisions.

4.1. Unauthorised payment transactions and authentication requirements

Appeal courts and the Supreme Court have had the opportunity in the last decade to frequently take a position on payment services, especially concerning unauthorised transactions.[30] The issues brought before the courts in recent years mainly concern home banking fraud schemes, while in the 90's the courts mainly debated liability for the loss, theft or misappropriation of debit and credit cards.[31]

---

[30] For a review of the Portuguese case law on payment services and unauthorized transactions over the years, see our works *As transferências electrónicas de fundos e os cartões de débito. Alguns problemas jurídicos relacionados com as operações de levantamento de numerário e de pagamento por meios electrónicos,* Coimbra, Livraria Almedina, 1999, p. 229 ff.; "Os cartões bancários e as cláusulas contratuais gerais na jurisprudência portuguesa e espanhola. Breve análise da jurisprudência mais recente dos tribunais superiores portugueses e espanhóis em matéria de cláusulas contratuais gerais inseridas nos contratos de utilização de cartões bancários", *in Revista de Direito e Estudos Sociais,* XLIII, 1, Lisboa, Verbo, 2002, pp. 55-91; "A repartição dos prejuízos decorrentes de operações fraudulentas de banca electrónica (*home banking*), Anotação ao Acórdão do Tribunal da Relação de Guimarães de 23.10.2012, Proc. 305/09", *in Cadernos de Direito Privado*, no 41, Janeiro/Março 2013, pp. 45-69; "As operações fraudulentas de *home banking* na jurisprudência recente — Ac. do STJ de 18.12.2013, Proc. 6479/09", *in Cadernos de Direito Privado*, no 49, Janeiro/Março 2015, pp. 9-33; and "O *phishing* de dados bancários e o *pharming* de contas. Análise jurisprudencial", *in III Congresso de Direito Bancário*, [L. M. Pestana de Vasconcelos (coord.)], Coimbra, Livraria Almedina, 2018, pp. 405-432.

[31] M. R. Guimarães, "Os cartões bancários e as cláusulas contratuais gerais na jurisprudência portuguesa e espanhola...", pp. 70-82, and "O *phishing* de dados bancários e o *pharming* de contas...", pp. 418-428. For further developments on

Unauthorised home banking transactions are caused either by breaking strong dynamic authentication through mobile phones, when the user downloads malware software to his or her mobile phone after disclosing the phone number and model on an unauthentic bank website, or, more frequently, using non-dynamic authentication, by means of code combinations pre-printed on plastic cards, that the user has previously revealed on a cloned website, in the belief that the access is genuine.[32] Invariably, the service provider refuses to reimburse the user for the loss claimed, and seldom can the funds be recovered from the third person that gave the payment order.[33]

Portuguese case law on home banking unauthorized payments, see M. C. França Barreira, "Home banking; a repartição dos prejuízos decorrentes de fraude informática", *in RED — Revista Electrónica de Direito*, no 3, Outubro 2015, Porto, CIJE/FDUP, p. 30 ff., <http://www.cije.up.pt/revistared> (25.01.2020).

[32] "Strong authentication" is defined by PSD2 article 4 (30) as "an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data". The same definition has been adopted by Decree-Law 91/2018, article 2 (d). Decree-Law 91/2018 article 104 (2) provides that for electronic remote payment transactions the required strong customer authentication must include elements "which dynamically link the transaction to a specific amount and a specific payee". See also articles 4 (1) and 5 (1) of Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication [C/2017/7782], *OJ* L 69, 13.3.2018, pp. 23-43.

[33] According to PSD2, article 73 (1), and Decree-Law 91/2018, article 114 (1), the service provider must refund the user the amount of the unauthorised payment transaction immediately, "and in any event no later than by the end of the following business day", not only after being notified by the user, but also after *noting itself* the anomalous transaction, the law requiring a positive act and not just a reactive attitude from the bank as before. The bank can only avoid the immediate refund "where there is a high suspicion of an unauthorised transaction resulting from fraudulent behaviour *by the payment service user*" — as stated in recital 71,

Traditionally, before PSD 1, Portuguese courts used to solve all the matters concerning payment services with the Portuguese Unfair Contractual Terms Act, Decree-Law 446/85 of 25 October. The parties' liability was distributed according to the contractual terms, closely supervised by the Unfair Contractual Terms Act, its black and grey lists of unfair terms and by the *bona fide* principle, and integrated with the general rules of the civil code. After 2007, and even after the 2009 Act, the same direction was followed and it took several years for the national courts to incorporate the new PSD rules, adopted by Decree-Law 317/2009.

Statistically, the majority of the sentences from Portuguese appeal courts have decided in favour of the users with two very different arguments: either because the users negligent conduct was not proven, namely that they made their access credentials available to a third person; or providing access credentials, in the particular circumstances, was not considered as grossly negligent behaviour.[34] It is not possible, however, to describe a tendency based on the data we have, since the proof that was supplied in each case was different, and, also, authentication methods differed in each case.

At the beginning of the last decade the majority of unauthorized home banking payments occurred as a result of non-dynamic authentication methods based simply on the use of elements of

---

although article 73 (1) does not refer to the authorship of the fraud; differently, the Portuguese Act refers to the fraudulent behaviour by "the payer" (*ordenante*): see *supra* note 27 —, and communicates those grounds to the relevant national authority, in writing. This last solution was already sustained by some authors in the context of PSD 1, based on an argument of reasonableness. In Portuguese literature see P. Guerra, "A realização de operações de pagamento não autorizadas e a tutela do utilizador de serviços de pagamento em face do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica", *in RED — Revista Electrónica de Direito*, no 2, Junho 2016, Porto, CIJE/FDUP, pp. 28-30, <http://www.cije.up.pt/revistared> (25.01.2020).

[34] M. R. Guimarães, "O *phishing* de dados bancários e o *pharming* de contas...", pp. 427-428.

knowledge (usernames and passwords) and possession (plastic cards with a printed ruled grid with numerical combinations, obtained by horizontal and vertical lines, in a *Battleship* style). Courts discussed the scope of the confidentiality and security duty imposed on the user.

The sentence of *Tribunal da Relação de Coimbra* of 2 February 2016 decided that the fact that a partner revealed credentials that gave access to a company e-banking account to another partner when the former left the company was not considered grossly negligent behaviour since the credentials never left the "sphere" of the company that held the account nor were disclosed to third parties.[35]

Furthermore, the sentence of the Portuguese Supreme Court (*Supremo Tribunal de Justiça*) of 14 December 2016 stated that communicating the security credentials to an accountant, in charge of the user's accounting, is compatible with the diligence of an average, reasonable, person and, therefore, diligent behaviour.[36]

At the same time, the fact that the user entered all his/hers access code coordinates (which were printed on a plastic card) on a corrupted bank website, in the belief that he/she was accessing his/hers home banking account, was taken as a breach of the contract when proved that the bank had displayed security alerts on its site clarifying that no more than two coordinates would be requested to perform the intended operations.[37] Still, other sentences have pointed out that when the unauthorised payments took place, several years before, when this type of fraud scams were not well known, it was considered plausible to be asked for all the code coordinates

[35] Sentence of *Tribunal da Relação de Coimbra* of 2 February 2016 (Rapporteur Arlindo Oliveira), *in* <http://www.dgsi.pt>. All the sentences quoted in the text can be found in the same website and were last consulted on 25 January 2020.

[36] Sentence of *Supremo Tribunal de Justiça* of 14 December 2016 (Rapporteur Pinto de Almeida).

[37] See, among others, the sentence of *Tribunal da Relação de Évora* of 25 June 2015 (Rapporteur Cristina Cerdeira).

pre-printed on the plastic cards issued by the bank, so the users' behaviours could not be seen as grossly negligent conducts.[38]

It is clear that today's home banking service providers draw their customers' attention to the schemes that were perpetrated almost ten years ago but they are not so up to date with the types of fraudulent access that are potentially being carried out now and will be judged by the courts in the future.[39] With regard to new cases of fraud, we will have to analyse the conduct of users focusing on the information available at the time when the unauthorised operation was carried out and not in the light of the knowledge acquired and widely disclosed at a later date.

Even so, the *Tribunal da Relação de Guimarães*, in its sentence of 10 July 2019, looking at facts that had taken place in 2017 — 60 unauthorized payments made between 4 and 7 January 2017 — considered the user not liable. The fraud was also performed with a coordinates card and the Court assumed that despite the fact that the user might be culpable of violating her obligations of care

---

[38] Sentence of *Tribunal da Relação de Guimarães* of 17 December 2014 (Rapporteur Fernando Fernandes Freitas): "That is why Banks, faced with the reiteration of these situations, found themselves in need of refining fraud alerts — from a passive attitude of the user, who was required to consult a folder with security rules (which is not compatible with pressure situations such as those we face daily) to an active position, "forcing" the user to heed warnings — but these measures, rather than being reactive, should have been preventive, knowing that hackers are resourceful and patient." See also sentence of *Tribunal da Relação do Porto* of 29 April 2014 (Rapporteur Francisco Matos) and sentence of *Tribunal da Relação de Lisboa* of 15 March 2016 (Rapporteur Rijo Ferreira). In this last sentence the court said that "Nor, by the very nature of things, can one qualify the conduct of those who provide security credentials subject to a fraudulent practice ('phishing','pharming', 'keylogging') as seriously negligent. These fraudulent practices are carried out because a large number of people are deceived through them and not just the extremely careless or unwary; and a conduct that is qualified as grossly negligent, cannot be likely to be carried out by a significant number of average men."

[39] Also S. Mason, "Electronic banking and how courts approach the evidence", *in Computer Law and Security Review*, no 29, 2013, p. 147, points out that "thieves are ahead of the game (...) and the weaknesses they exploit now will not be known for some time (...)."

when, regardless of the service provider's notices, she disclosed all the card coordinates on a cloned website, all the circumstances of the case should be taken into account as recommended in recital 33 of PSD 1, concluding that the user's conduct was not *grossly* negligent. The Court pointed out that despite the warnings on how to correctly use the numbers of the coordinates card to access the home banking service, this would not in most cases be enough to qualify the negligence of a victim of fraud as "gross", placing gross negligence at the level of "unforgivable error, inexplicable inattention, inexcusable negligence". [40]

The Court considered it significant that it is not uncommon for users only to use their home banking system to consult their respective balances, these being an extremely vulnerable group due to their computer illiteracy. For them, the warnings addressed to the users of the service are inadequate and other types of warnings, possibly of a personalized nature, should be implemented by the service provider in order to effectively fulfil its obligation to guarantee the security of the system.[41]

Whatever the case, according to the new rules on the payer's liability for unauthorised payment transactions introduced by PSD2, and regardless of the more or less diligent behaviour the payer adopts or the fulfilment of the information and alert duties by the service provider, the liability for unauthorised payments will always rest with the service provider when non-dynamic authentication is accepted. And that is the case with the authentication based on combinations of numbers pre-printed in a plastic card, unable to "dynamically link the transaction to a specific amount and a specific payee". If for the purposes of the payer's authentication, the payment service provider only relies on the combination of a user name and a security code and the knowledge of several combinations of

---

[40] Sentence of *Tribunal da Relação de Guimarães* of 10 July 2019 (Rapporteur Margarida Sousa).

[41] *Idem.*

numbers that are pre-printed on a plastic card issued when the home banking contract is concluded, it will have to bear the losses caused by unauthorised payment orders given by third parties, unless the user has acted fraudulently.[42] The same solution will apply to credit card payments on e-commerce transactions, when the user authentication is based only on the credit card number, expiry date and verification code, all printed on the same plastic card.[43]

More sophisticated fraud schemes were operated through mobile phones, acting as authentication devices that generate the dynamic link between the transaction, the amount of the payment and the payee, necessary for the strong authentication that remote payments require. And in these cases — significantly less frequent than the unauthorized payments made without this authentication —, the pertinence of the distinction between gross and simple negligent conducts remains.

4.2. Gross negligence, simple negligence and burden of proof

In recent years the Portuguese appeal courts have established patterns regarding ordinary or simple negligence and gross negligence conducts, which have developed over the years, taking in account, as we have pointed out *supra*, the alerts on security conducts and fraud schemes given by the banks and increasing the due diligence standards imposed on the user.

Unauthorized remote payments made with strong authentication, namely introducing a security code generated for the transaction and sent to the user's mobile phone, are most commonly the result

[42] See PSD2, article 74 (2), and Decree-Law 91/2018, article 115 (5). As M. Donnelly, "Payments in the digital market...", p. 836, puts it, this provision is "one of the most striking innovations in PSD II."

[43] R. Steennot, "Reduced payer's liability for unauthorized payment transactions under second Payment Services Directive (PSD2)", p. 960, points out that the user also will not be liable if the absence of strong authentication is a consequence of the exemptions of articles 10 ff. of the Commission Delegated Regulation 2018/389 of 27 November 2017.

of a malware infection. In the case that generated the sentence of *Tribunal da Relação do Porto* of 7 October 2014, the user was asked to download a programme for mobile phones when accessing what he thought was his home banking account and to introduce his phone number and model. He then downloaded the software on his phone. The Appeal Court of Porto stated that "in this case, it was necessary for the [user] to be a very experienced person and very knowledgeable of the means of navigation in an electronic environment so that he could be suspicious of the bait that was launched in the proven circumstances. However, the Appellant Bank, when it contracts the home banking service with its clients does not require these skills."[44]

In a similar case, evaluated in 2019, the Court argued that the user, in the belief that he was on the bank's trustworthy page, simply introduced the data requested there, without being informed about what data could or should be used to access the site, and what other elements, under no circumstances, should be provided, such as the mobile phone number or ID.[45] The Court decided that the user did not act with gross negligence and not even with simple negligence although it may appear that the data that had been requested from the user was different from that which was usually required when accessing the bank portal, with no proof from the bank that they had provided this information.

Recent sentences have been clear in the sense that the payment service provider has the burden of proof of the occurrence of a simple negligent, gross negligent or intentionally faulty behaviour by the user, moving towards the new requirement introduced in PSD2, article 72 (2), and, in Portugal, in Decree-Law 91/2018, article 113 (4).[46]

---

[44] Sentence of *Tribunal da Relação do Porto* of 7 October 2014 (Rapporteur Ana Lucinda Cabral), summary III.

[45] Sentence of *Tribunal da Relação de Coimbra* of 15 January 2019 (Rapporteur Moreira do Carmo).

[46] Both articles state that the service provider must provide "supporting evidence" to prove fraud or gross negligence of the user. As R. Steennot, "Reduced payer's liability for unauthorized payment transactions under second Payment

It has been understood that the user acts without any fault or negligence when, using the home banking services, he or she is the victim of a computer attack — namely through the "pharming" technique —, resulting in an unauthorized transfer of funds, when no further proof is achieved.[47]

As was explained by *Tribunal da Relação de Lisboa* in 2018,[48] the implication of the burden of proof rules is that the risks for the normal use of the system are borne by the payment service provider, which the Court considered "perfectly normal" since the bank will gain the greatest economic benefit from its proper functioning. On the other hand, the Court also stated that the bank's burden of proof that payment transactions have not been affected by technical faults or any other shortcomings, and the fact that the correct registration of the payment is not necessarily sufficient in itself to prove that the transaction was authorized by the user, that he or she acted fraudulently or they failed to fulfil, with intent or gross negligence, one or more of their obligations, is the consequence of the simple reason that the user could not be placed in the need to prove the operability and regular functioning of a complex computer system owned by the bank and which the customer does not master.[49]

Services Directive (PSD2)", p. 962, points out, "the importance of this clarification should not be underestimated", having the effect to proscribe presumptions of gross negligence based on the mere assumption that if the payment instrument was correctly used the user must have authorized the payment or boosted it with his gross negligence.

[47] See, among others, the recent sentence of *Tribunal da Relação do Porto* of 4 June 2019 (Rapporteur Alexandra Pelayo). About Italian case law, described by the Author as "*alquanto oscillante*", see V. De Stasio, *Ordine di pagamento non autorizzato e restituzione della moneta*, Giuffrè Editore, Milano, 2016, pp. 142-143, particularly note 96.

[48] Sentence of *Tribunal da Relação de Lisboa* of 6 November 2018 (Rapporteur Ana Pessoa).

[49] *Idem.* The formula "the use of a payment instrument recorded by the payment service provider (...) *shall in itself not necessarily be sufficient* to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or

In recent years, in a rare case of unauthorized credit card payments, the same *Tribunal da Relação de Lisboa* stated that "in case of improper use of a credit card, the respective holder who claims not to have authorized the transaction is not charged with any presumption of guilt of not complying with his custody duties".[50] On the alleged impossibility of the payments having been made without the card verification value (CVV) code — and, therefore, without the user's negligence —, the *Tribunal da Relação de Lisboa* said that the bank's witnesses who testified "revealed some knowledge due to the functions performed, and issued opinions on the reasons for assuming that the movements in question had been carried out by someone with access to the card, respective data, and data of the holder. But this is an assumption, which is not confirmed with the minimum security required by other evidential elements, and therefore does not constitute adequate evidence to demonstrate that the author acted with gross negligence".[51] The Court devalued the "experience of life" and the opinions on what is assumed as the "normal course of events", favouring the user and the presumption of the user's innocence.[52]

---

failed with intent or gross negligence to fulfil one or more of [his] obligations", already used on PSD 1, is seen in Spain by J. M. López Jiménez, *Comentarios a la Ley de servicios de pago*, Barcelona, Bosch, 2011, p. 595, as a specific provision for payment cards, since the obligations under article 69 [PSD2; article 27 of Spanish first *Ley de Servicios de Pago*, the provision that is the subject to this observation] are, according to the Author, obligations typically related with the use of debit and credit cards. However, bearing in mind the broad definition of "payment instrument" adopted both in PSD 1 and 2, we cannot follow the Author's position. On PSD2 "payment instrument" definition, see B. Geva, "Payment Transactions under the E.U. Second Payment Services Directive—An Outsider's View", *in Texas International Law Journal*, Vol. 54:2, 2019, p. 228: "A card used with or without a personal code will satisfy this definition. Moreover, any agreed upon security procedure will be a 'payment instrument'".

[50] Sentence of *Tribunal da Relação de Lisboa* of 8 March 2018 (Rapporteur Ana Paula Carvalho).

[51] *Idem.*

[52] Suggesting that some courts reach incorrect decisions when bank customers claim the refund of unauthorized payments, based on the acceptance of unwarranted assumptions and, in general, a misunderstanding of the burden

Even so, with the new authentication and liability rules introduced by PSD2, the bank would have to prove that the user had acted fraudulently in order to avert its own liability, since the unauthorized payments were the consequence of credit card remote transactions, the bank not having required strong customer authentication of the user.

4.4. Monitoring security risks

In the last few years Portuguese appeal courts have been gaining awareness of the fact that banks must play an active role in monitoring payment orders, disclosing fraud schemes and sending alerts to their clients when an operation deviates from the user's "normal" behaviour. The banks must know their customers and their standards of conduct. Today this monitoring is done by computers that analyse patterns of transactions and their deviations depending on the geographical origin of the IP through which the account is accessed, time of access, value of operations, etc.

PSD 1 already allowed the bank to include in the framework contract the possibility of blocking a payment instrument for objective reasons of security or suspected fraud,[53] conditions that could be fulfilled whenever unusual operations due to their amounts,

---

of proof, see S. Mason, "Electronic banking and how courts approach the evidence", pp. 144-151. The Author, focusing on card transactions, points out that banks invariably claim that the customer acted with gross negligence despite being often incapable of producing sufficient evidence to prove their case. Mason further adds that "it is astounding that a judge would assume that the standard security systems used by the bank were effective" (p. 147) when "the effective imposition of the burden of proof might act to cause the banks to consider more carefully the avoidance of careless activities" (p. 150).

[53] This option has been maintained on PSD2, articles 52 (5) (c) 68 (2). According to M. J. da Costa Gomes, *Contratos Comerciais*, Coimbra, Livraria Almedina, 2012, pp. 242-243, this possibility of blocking the payment instrument comprises a real duty that results from the principle of good faith imposed on the service provider.

periodicity or volume took place, or operations originating in "suspicious" countries, and, therefore, likely to constitute situations of fraud.

The new directive moves forward on the payment service provider's duty to manage operational and security risks, imposing mitigation measures and control mechanisms, including "effective incident management procedures (...) for the detection and classification of major operational and security incidents".[54] At least on an annual basis, payment service providers must report updated information on operational and security risks and on the adequacy of the existing measures and control mechanisms.[55] They must also notify competent national authorities — in Portugal, *Banco de Portugal* — "without undue delay", in cases of major security incidents, as well as the service users, whenever the incidents may have an impact on their interests.[56]

In addition, Commission Delegated Regulation 2018/389 of 27 November 2017, on regulatory technical standards for strong customer authentication and common and secure open standards of communication, states that payment service providers shall have transaction monitoring mechanisms in place that enable them to detect unauthorised or fraudulent payment transactions.[57] Moreover, article 18 (2) of the same Commission Delegated Regulation 2018/389 defines several criteria that must be taken into account by the service provider when performing a real time risk analysis, namely the *(i)* abnormal spending or behavioural pattern of the payer; *(ii)* unusual information about the payer's device/software

---

[54] See PSD2, article 95 (1), and Decree-Law 91/2018, article 70 (1) (2). This key feature of PSD2 is pointed out by F. Mendes Correia, "Uma revolução permanente?...", pp. 402-403.

[55] See PSD2, article 95 (2), and Decree-Law 91/2018, article 70 (3).

[56] See PSD2, article 96 (1), and Decree-Law 91/2018, article 71 (1).

[57] Article 2 (1), Commission Delegated Regulation 2018/389 of 27 November 2017.

access; *(iii)* malware infection in any session of the authentication procedure; *(iv)* known fraud scenario in the provision of payment services; *(v)* abnormal location of the payer; and *(vi)* high-risk location of the payee.

Some of these standards have already been considered by Portuguese courts although not in a systematic way.

In the situation that generated the sentence of the *Relação de Évora* of 22 May 2014, which involved the unauthorized withdrawal of almost the entire balance of a home banking account, the user had never carried out any online payment before and only used the service to consult his account balance. The Court assumed that "the bank is aware that there is a pattern of conduct that can make the identity of the person who conducts it [the payment order] suspicious, so in the specific case the security rules should have made the bank collect additional elements before authorization, as it was a transfer of almost all the funds in the bank account, by a customer who had never carried out any transaction through the service over several years."[58]

In the same way, and also in 2014, the *Tribunal da Relação de Guimarães* stated that "with the IT resources available to them and the knowledge of the people who are their regular customers, it would be easy for the Banks to profile the user (as Google does in relation to the holders of email accounts), barring operations to whoever, due to late and unusual time, tries to make 'transfers' to third parties, or, for the repetition of unusual transfers in a short period of time, in short, everything that deviates from the normal pattern of use that the client has been revealing, thus contributing to a greater security of the system, that we want, as far as possible, armored."[59]

---

[58] Sentence of *Tribunal da Relação de Évora* of 22 May 2014 (Rapporteur Mata Ribeiro).

[59] Sentence of *Tribunal da Relação de Guimarães* of 17 December 2014 (Rapporteur Fernando Fernandes Freitas).

Nevertheless, in a situation judged in May 2012 the bank allowed two payment orders on subsequent days of 5,000 euros each, with the description "instalment motorboat" and "instalment vehicle", in a home banking account from a user who had never diverged from a pattern of small deposits and occasional withdrawals.[60] In this case it was the user who notified the bank concerning the unauthorized transactions, before the bank, realizing what had happened, managed to avoid a second payment. But the deviations from the user's standard behaviour seem to be clear in this case, imposing on the bank the obligation to notify its customer and confirm the originality of the transfer orders before proceeding with their execution, or, alternatively, to deny the transaction. This solution would be the natural outcome of the special relationship of trust established between the bank and its customer, based on the framework contract,[61] but the special monitoring duties that are now imposed on the bank will simplify court decisions whenever these duties are not fulfilled.

5. Final remarks

The new rules on payment services have introduced important changes in several key aspects of the previous regime, namely concerning new players that are now subject to payment service provisions, user's authentication, reimbursement of unauthorized payments, burden of proof of gross negligence or fraud and users' and service providers' liability for unauthorized transactions.

---

[60] Sentence of *Tribunal da Relação de Lisboa* of 24 May 2012 (Rapporteur Ezagüy Martins).

[61] M. R. Guimarães, "O *phishing* de dados bancários e o *pharming* de contas...", p. 417. The same position was assumed by R. S. Ribeiro de Lima, "A responsabilidade pela utilização abusiva on-line de instrumentos de pagamento eletrónico na jurisprudência portuguesa", *in RED — Revista Electrónica de Direito*, no 3, Outubro 2016, Porto, CIJE/FDUP, pp. 28-29, <http://www.cije.up.pt/revistared> (25.01.2020).

Based in this analysis of the new provisions, it can be said that Portugal generally complies with the 2015 Directive design, closely following the structure of PSD2 but also taking advantage of the discretion that was allowed to Member States in some crucial aspects such as limiting the user's liability for gross negligent behaviours.

Some national appeal courts have already mentioned the new legal framework that emerges from PSD2 and Decree-Law 91/2018. However, sentences of *Tribunal da Relação do Porto* of 8 March and 4 June 2019 both devalued the new law, noting that "it generally maintained the discipline and the regime in force since 2012".[62] The Court of Appeal of Guimarães, nevertheless, pointed out in a sentence of 10 July 2019 that the new law imposes additional requirements of strong authentication for the authorization of a payment transaction, being aware of the changes that this will mean when judging new facts.[63]

It is going to take some time before the new rules on unauthorised transactions will make a difference in concrete disputes over payment services, particularly before the Portuguese higher courts take a position on the solutions now found for e-commerce payments. Hopefully, the subtleness of some changes of strong practical impact will be quickly comprehended and courts will continue to play an important role in the protection of diligent payment service users and in the construction of a single European payments market.

[62] Sentences of *Tribunal da Relação do Porto* of 8 March and 4 June 2019 (Rapporteur Alexandra Pelayo).

[63] Sentence of *Tribunal da Relação de Guimarães* of 10 July 2019 (Rapporteur Margarida Sousa).

References

Barreira, Maria Carolina França, "Home banking; a repartição dos prejuízos decorrentes de fraude informática", *in RED — Revista Electrónica de Direito*, n.o 3, Outubro 2015, Porto, CIJE/FDUP, <http://www.cije.up.pt/revistared> (25.01.2020)

Correia, Francisco Mendes, "uma revolução permanente? A DSP 2 e o novo Direito dos Serviços de Pagamento", *in III Congresso de Direito Bancário*, [L. Miguel Pestana de Vasconcelos (coord.)], Coimbra, Livraria Almedina, 2018, pp. 385-404

De Stasio, Vincenzo, *Ordine di pagamento non autorizzato e restituzione della moneta*, Giuffrè Editore, Milano, 2016

Donnelly, Mary, "Payments in the digital market: Evaluating the contribution of Payment Services Directive II", *in Computer Law & Security Review*, no 32, 2016, pp. 827-839

Geva, Benjamin, "Payment Transactions under the E.U. Second Payment Services Directive—An Outsider's View", *in Texas International Law Journal*, Vol. 54:2, 2019, pp. 211-243

Gomes, M. Januário da Costa, *Contratos Comerciais*, Coimbra, Livraria Almedina, 2012

Guerra, Patrícia, "A realização de operações de pagamento não autorizadas e a tutela do utilizador de serviços de pagamento em face do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica", *in RED — Revista Electrónica de Direito*, no 2, Junho 2016, Porto, CIJE/FDUP, <http://www.cije.up.pt/revistared> (25.01.2020).

Guimarães, Maria Raquel, *As transferências electrónicas de fundos e os cartões de débito. Alguns problemas jurídicos relacionados com as operações de levantamento de numerário e de pagamento por meios electrónicos,* Coimbra, Livraria Almedina, 1999

— "Os cartões bancários e as cláusulas contratuais gerais na jurisprudência portuguesa e espanhola. Breve análise da jurisprudência mais recente dos tribunais superiores portugueses e espanhóis em matéria de cláusulas contratuais gerais inseridas nos contratos de utilização de cartões bancários", *in Revista de Direito e Estudos Sociais,* XLIII, 1, Lisboa, Verbo, 2002, pp. 55-91

— "The debit and credit card framework contract and its influence on European legislative initiatives", *in InDret Comparado*, *Revista para el Análisis del Derecho*, no 2, 2012, <http://www.indret.com/pdf/892_en.pdf> (25.01.2020)

— "A repartição dos prejuízos decorrentes de operações fraudulentas de banca electrónica (*home banking*), Anotação ao Acórdão do Tribunal da Relação de Guimarães de 23.10.2012, Proc. 305/09", *in Cadernos de Direito Privado*, no 41, Janeiro/Março 2013, pp. 45-69

— "As operações fraudulentas de *home banking* na jurisprudência recente — Ac. do STJ de 18.12.2013, Proc. 6479/09", *in Cadernos de Direito Privado*, no 49, Janeiro/Março 2015, pp. 9-33

— "Los medios de pago en el derecho europeo y en los instrumentos europeos de armonización del derecho privado", *in Banca, Borsa, Titoli di Credito*, vol. 70, no 4, Milano, Giuffrè Editore, 2017, pp. 555-575

— "O phishing de dados bancários e o pharming de contas. Análise jurisprudencial", *in III Congresso de Direito Bancário*, [L. Miguel Pestana de Vasconcelos (coord.)], Coimbra, Livraria Almedina, 2018, pp. 405-432

Lima, Raquel Sofia Ribeiro de, "A responsabilidade pela utilização abusiva on-line de instrumentos de pagamento eletrónico na jurisprudência portuguesa", *in RED — Revista Electrónica de Direito*, no 3, Outubro 2016, Porto, CIJE/FDUP, <http://www.cije.up.pt/revistared> (25.01.2020)

López Jiménez, José María, *Comentarios a la Ley de servicios de pago*, Barcelona, Bosch, 2011

Mason, Stephen, "Electronic banking and how courts approach the evidence", *in Computer Law & Security Review*, no 29, 2013, pp. 144-151

Pacheco Jiménez, Mª Nieves, "La nueva directiva 2015/2366 de servicios de pago en el mercado interior", *in Revista CESCO de Derecho de Consumo*, no 16/2016, pp. 139-143, <https://revista.uclm.es/index.php/cesco> (25.01.2020)

Steennot, Reinhard, "Reduced payer's liability for unauthorized payment transactions under second Payment Services Directive (PSD2)", *in Computer Law & Security Review*, no 34, 2018, pp. 954-964

Wolters, P.T.J / Jacobs, B.P.F, "The security of access to accounts under PSD2", *in Computer Law & Security Review*, no 35, 2019, pp. 29-41

Reinhard Steennot[1]
(Professor Ghent University, Financial Law Institute)

LIABILITY FOR UNAUTHORIZED PAYMENT TRANSACTIONS: THE TRANSPOSITION OF PSD2 IN BELGIUM

I. Introduction

1. Within the EU, payment services are dealt with by the second Payment Services Directive (PSD2)[2] of 2015. The replacement of the first Payment Services Directive (PSD1)[3] had become a necessity because of the technological innovation on the payment markets, including the increasing use of Internet-banking and mobile banking and the introduction of new types of services, such as payment initiation services and account information services[4]. Important objectives of the Directive are among other things to increase security

[1] Financial Law Institute, Ghent University - Consumer Law Institute, Ghent & Antwerp University.

[2] 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 [2015] OJ L 337/35.

[3] 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 [2007] OJ L 319/1. On the liability regime in PSD1 see for example: R. Steennot, "Allocation of liability in case of fraudulent use of an electronic payment instrument: the new directive on payment services in the internal market" *Computer Law & Security Review*, 2008, 555.

[4] Recital 3 PSD2.

of payments and to strengthen consumer protection[5]. Unauthorized payment transactions should be prevented as much as possible (in particular by requiring strong customer authentication in many occasions). If, despite all security measures taken unauthorized transactions do occur, the risk for consumers should be kept to a minimum, unless when the consumer acted fraudulently or failed to meet his or her obligations with intent or gross negligence.

2. When implementing PSD1, the Belgian legislator did not limit itself to a mere copy paste of the Directive's provisions. It used the possibility, offered by PSD1[6], to further reduce payer's liability in particular circumstances. When transposing PSD2, the Belgian legislator however stuck to the Directive's text (with the exception of the rule clearly imposing the burden of proof of gross negligence on the payment service provider (PSP)). The objective of this paper is two-fold: on the one hand it aims to find out whether the increased protection offered by PSD2 fully compensates for the abolition of the old Belgian liability rules, on the other hand it focuses on the interpretation of some of the liability rules in Belgium case law.

Since (published) court decisions[7] are rather limited in number, the recommendations[8] of the Ombudsman in financial services (Ombudsfin)[9] will receive quite a lot of attention in this article. Figures show that the amount of admissible complaints relating to payments has substantially increased over the last few years, from 163 in 2014, to 454 in 2018[10].

---

[5] Recitals 6 and 7 PSD2.

[6] Article 61.3 PSD1.

[7] In Belgium, not all court decisions are published online (except for those of the highest courts).

[8] The decisions of the Ombudsman in financial services are not binding upon the parties.

[9] Annual reports of Ombudsfin, as well as the recommendations of the expert panel can be accessed online: https://www.ombudsfin.be/fr/particuliers/publications/rapports-annuels/.

[10] Ombudsfin, Annual Report 2018, https://www.ombudsfin.be/sites/default/files/RA-Ombudsfin%202018.pdf (p. 12).

Remarkable is also that claims concerning payments accounted for nearly half of the total of admissible complaints in 2018[11]. Whereas originally, disputes most often related to the unauthorized use of payment cards and the absence or existence of gross negligence, cases relating to phishing, vishing and other new types of fraud have become much more important the last few years. With these new types of fraud the amount of damages that PSUs suffer, has also substantially increased. Some PSUs have lost thousands of euros, in particular in cases where scammers have been able to install mobile payment applications (in particular mobile banking apps) on their own smartphone, and using these apps, have been able to even get access to funds on savings accounts.

II. Transposition in Belgium

3.PSD2 was transposed into Belgian law by means of two individual acts. The public law provisions were implemented in the Act of 11 March 2018 relating to the legal status of and the oversight on payment institutions and Electronic money institutions, the access to the provision of payment services, the issue of Electronic money and payment systems[12]. With the exception of some provisions, this act entered into force on 26 March 2018. The private law provisions were transposed in Book VII of the Code of Economic Law (CEL)[13],

[11] Ombudsfin, Annual Report 2018, https://www.ombudsfin.be/sites/default/files/RA-Ombudsfin%202018.pdf (p. 12).

[12] Official Journal (Moniteur) 26 March 2018.

[13] See: Act of 19 July 2018 concerning the change and introduction of rules on payment services in several books of the Code of Economic Law, Official Journal (Moniteur) 30 July 2018. Book VII of the Code of Economic Law also includes rules on payment accounts (transposing the Payments Accounts Directive), as well as rules on consumer and mortgage credits (transposing the Consumer Credit and the Mortgage Credit Directive).

in which the PSD1 principles were incorporated in 2014[14]. The new rules entered into force on 9 August 2018, several months too late.

4. As PSD1, PSD2 is based on maximum harmonization[15]. Therefore, Member States transposing PSD2 into their national legislation cannot offer any additional protection to PSUs, unless where explicitly stated otherwise in the Directive itself[16]. In the context of unauthorized payment transactions article 61, 63 and 74 PSD2 are of particular importance.

5. Article 61 PSD2 makes it possible to protect *microenterprises* in the same way as consumers. This finding is important since most provisions on unauthorized payment transactions are only mandatory in the relation to consumers[17]. Unfortunately, the Belgian legislator did not use the possibility offered by article 61 PSD2, arguing that professionals should be able to negotiate the contractual terms[18]. The argument is not very convincing, since PSPs (generally) use a take it or leave it approach when it comes to standard terms[19]. Moreover, Belgian (micro)enterprises will not be able to invoke any other

---

[14] Act of 19 April 2014 concerning the incorporation of Book VII "Payment and credit services" in the Code of Economic Law, Official Journal (Moniteur) 28 May 2014. Before that, the PSD1 provisions could be found in a separate act: Act of 10 December 2009 concerning payment services, Official Journal (Moniteur) 15 January 2010.

[15] Article 107 PSD2.

[16] However, full harmonization does not prevent Member States to extend the scope of application, neither to introduce provisions on topics that do not fall within the field harmonized by the Directive (see e.g.: ECJ 12 July 2012, Case C-602/10, *Volksbank Romania*, ECLI:EU:C:2012:443).

[17] Article 61.1 PSD2.

[18] Explanatory memorandum, Chamber of Representatives, Doc. 52, 2179/001, 13 (https://www.dekamer.be/FLWB/PDF/52/2179/52K2179001.pdf).

[19] I. De Poorter, "De wet betreffende de betalingsdiensten leidt tot een betere bescherming van de consument", *Rechtskundig Weekblad* 2011, 1332. See also : P. Berger & S. Landuyt, "Toepassingsgebied van de wet betalingsdiensten en de wet betalingsinstellingen", in IFR (ed.), *Financiële regulering in de kering*, Antwerpen, Intersentia, 2012, 131, according to which a more convincing argument would be that Belgian law is not familiar with the concept of a microenterprise.

protection against unfair contract terms. On the one hand they cannot be considered consumers[20]. On the other hand, the Act of 4 April 2019[21], which among other things prohibits terms creating a significant imbalance between the rights and obligations of the contractual parties in B2B contracts[22], does not apply to contracts concerning financial services, such as payment services[23].

6. According to article 63.1 PSD2, PSPs and PSUs can agree that the articles 72, 73 and 74 (1) and (3) PSD2 do not apply to *low value payment instruments* if the payment instrument is used anonymously or the payments service provider is not in a position for other reasons which are intrinsic to the payment instrument to prove that a payment transaction was authorized. Low value payment instruments are payment instruments which, according to the framework contract, solely concern individual payment transactions not exceeding 30 euro or which either have a spending limit of 150 euro, or store funds which do not exceed 150 euro at any time. Article 63.2 PSD2 enables Member States to either reduce or double these amounts. Also Member States can increase them for prepaid instruments up to 500 euro. The Belgian legislator did not use any of these possibilities[24], but in the future the amounts can be adapted by Royal Decree[25].

---

[20] Legal persons, as well as natural persons using payment instruments for professional purposes cannot be considered consumers. It is however accepted that natural persons acting for *mainly* private purposes are consumers (although not explicitly stated in the definition in article I.1, 2° Code of Economic Law). See: Cassation Court 9 March 2018, C.17.0065.F/1, www.cass.be, *Rechtskundig Weekblad* 2019-2020, 390 (in the context of consumer sales) and Cassation Court 17 October 2014, C.13.04.00, www.cass.be, *Bank en Financieel Recht* 2014, 324 (in the context of consumer credit).

[21] Act of 4 April 2019 on the amendment of the Code of Economic Law with regard to misuse of economic dependence, unfair contract terms and unfair market practices between companies, Official Journal (Moniteur) 24 May 2019.

[22] Article VI.91/3 CEL.

[23] Article VI.91/1 CEL.

[24] Article VII.31 §1, 2° CEL.

[25] Article VII.31 §2 CEL.

Article 63.3 PSD2 implies that article 73 and 74 PSD2 do not apply to *Electronic money* if the PSP does not have the ability to freeze the payment account to which the Electronic money is stored or block the payment instrument. It entitles the Member States to limit this derogation to Electronic money accounts or to Electronic money instruments of a certain value. This possibility has been used by the Belgian legislator, applying the same limitations as those set with regard to low value payment instruments[26].

7. Article 74.1 PSD2 determines that where the payer has neither acted fraudulently nor intentionally failed to fulfil its obligations, Member States may *further reduce the payer's liability*, as determined by the Directive, taking into account in particular the nature of the personalized security credential and the specific circumstances under which the payment instrument was lost, stolen or misappropriated. As already mentioned, the Belgian legislator did not take this opportunity. Clearly the Belgian legislator believed that the new liability rules in PSD2 (offering more protection than those embedded in PSD1) sufficiently protect the PSU. As it will be shown, the new rules indeed offer additional protection in some cases, in other cases however they don't or at least not necessarily.

III. Concept of unauthorized payment transactions

8. A payment transaction is only authorized when the PSU has given his consent to the transaction[27]. Normally, consent is given prior to a payment transaction, but, if agreed by the payer and the PSP, transactions can also be ratified or approved afterwards. Consent must be given in the form and using the procedure agreed by the parties, usually in the framework contract (e.g. by providing login and password, communicating credit card details or scanning a QR-code and a PIN).

[26] Article VII.31 §4 CEL.

[27] Article 64 PSD2, article VII.32 CEL.

9. The question arises whether it is up to the PSU to prove that he did not authorize a payment transaction, or up to the PSP to prove that the PSU did so. As PSD2[28], Belgian law[29] contains two provisions in this regard: 1) Where a PSU denies having *authorized* a transaction, it is up to the PSP to prove that the transaction was *authenticated*[30]; 2) The mere use of the payment instrument recorded by the PSP (or the payment initiation service provider) is in itself not necessarily sufficient to prove that the payment transaction was authorized by the payer.

The importance of the latter rule cannot be underestimated, since it prevents that all transactions for which the personalized security credentials have been used are automatically considered authorized transactions. However, this provision does not imply that the burden of proof regarding the (un)authorized nature of the transactions is imposed entirely on the PSP. After it has become clear that a transaction was authenticated (i.e. the payment instrument has been used), the payer will first need to make it plausible that he at least did not initiate the transaction himself[31].

---

[28] Article 72 PSD2.

[29] Article VII.42 CEL.

[30] Authentication means a procedure which allows the PSP to verify the identity of a PSU or the validity of the use of a specific instrument, including the use of the user's personalized security credentials (article 4 (29) PSD2 and article I.9, 11° CEL). Personalized security credentials are personalized features provided by the PSP to a PSU for the purposes of authentication (art. 4 (31) PSD2 and article I.9, 33/17° CEL). They include for example passwords, PIN's, digital signatures and biometrical data.

If the payment transaction is initiated through a payment initiation service provider, the burden will be on the payment initiation service provider to prove, within its sphere of competence, that the payment transaction was *authenticated*.

[31] Ombudsfin 19 March 2019, nr. 2018.3288; Ombudsfin 18 December 2018, nr. 2018.1847; T. Baes, "Aansprakelijkheid bij uitvoeringsincidenten in het betalingsverkeer", in IFR (ed.), *Financiële Regulering in de kering*, Antwerpen, Intersentia, 2012, 169-170.

10. In general, it is quite easy – at least from a theoretical point of view – to make a distinction between authorized and unauthorized payment transactions. However, in some situations it becomes more difficult to do so. For example, suppose that a payer originally authorizes a payment transaction but the beneficiary (and the amount) are changed afterwards by a third party acting fraudulently. For instance, reference can be made to a case where the payer initiated a payment transaction through a banking website, after sharing his computer via *TeamViewer* with a third person who contacted him by phone and pretended to be a Microsoft employee. Once the transaction (with the claimed objective of making a payment to Microsoft) was initiated, the scammer changed the beneficiary and the amount of the transfer. Ombudsfin decided that such a transaction can indeed be considered unauthorized, since the payer did not consent to that specific payment transaction[32].

IV. Allocation of liability

11. When unauthorized payment transactions have taken place, it is often impossible to recover the funds from the person that has initiated the transaction (since that person can often not be identified or found). In such a situation, the question arises who can be held liable for the unauthorized transactions. Must the PSU or the PSP bear the risk?

§ 1 Scope: Payment transactions and payment instruments

12. As PSD2[33], Belgian law makes a distinction between unauthorized payment transactions in general and the unauthorized use of a payment instrument in particular[34]. Payment instruments are personalized devices and / or sets of procedures agreed between the

[32] Ombudsfin 19 September 2017, nr. 2017.1889.

[33] Article 73 and 74 PSD2.

[34] Article VII.43 and VII.44 CEL.

PSU and the PSP in order to initiate a payment order[35]. According to the ECJ every set of procedures, agreed between the PSU and the PSP, and used by the PSU in order to initiate a payment order, can be considered a payment instrument. These procedures do not need to be personalized[36]. They include for example mobile banking apps[37], but also credit transfers initiated in writing.

13. Taking into account the definition of a payment instrument and its wide interpretation by the ECJ, nearly all unauthorized payments will take place through the unauthorized use of a payment instrument. Equally important is that one device might include several payment instruments. For example on a mobile phone, several payments apps can be installed. These payment apps must then be considered different payment instruments. Therefore, the loss or theft of one device can lead to the unauthorized use of several payment instruments[38].

§ 2 Obligation of PSPs to provisionally credit the payer's account

14. When a payer notifies the PSP that an unauthorized payment transaction has taken place, the payer's PSP must refund the payer immediately, and in any event no later than by the end of the following business day. Only when PSPs have reasonable grounds for suspecting fraud they can suspend reimbursement. In order to avoid that PSPs conclude too easily to the existence of fraud, these grounds must be communicated in writing to the Ministry of Economic affairs[39]. The obligation to reimburse the payer is only

---

[35] Article 4 (14) PSD2 and article I.9, 10° CEL.

[36] ECJ 9 April 2014, Case C-616/11, *T-Mobile Austria*, ECLI:EU:C:2014:242.

[37] See also: Ombudsfin 18 June 2019, nr. 2019.734.

[38] R. Steennot & J. Goetghebuer, "Bescherming van de consument bij niet-toegestane mobiele betalingstransacties", in *Digitalisering van het recht en consumentenbescherming",* Antwerp, Intersentia 2019, 208-209.

[39] Article VII.43 §1 CEL.

provisional. If later on it becomes clear that the payer is (partly) liable, the PSP can reclaim the amount reimbursed[40].

Several cases submitted to Ombudsfin show that Belgian PSPs do not always comply with this requirement[41]. PSPs fear that they will not be able to recover the reimbursed amounts from the payer, if at a later stage it is found that the payer is liable. This behaviour is stimulated by the lack of a specific civil remedy, that payers can invoke if PSPs do not comply with this rule. In the absence of specific civil law remedies, it is up to the Economic Inspection, which is the supervising authority in this regard, to use its investigating and sanctioning powers (Book XV CEL) in order to force PSPs to comply with this obligation.

15. It is important to emphasize that this obligation to provisionally reimburse the payer also applies if the unauthorized transactions have been initiated through a payment initiation service or by credit card.

§ 3 Final allocation of liability

16. The basic liability regime makes a distinction between transactions that took place after notification of loss, theft or misappropriation of the payment instrument and transactions that took place before such notification. On the one hand, the payer cannot be held liable for transactions taking place after notification (unless when he acted fraudulently)[42]. On the other hand, the payer is liable for transactions that occurred before notification. However, the payer's liability is limited up to 50 euro, unless when he failed

[40] Y. Gérard, "L'utilisation frauduleuse des instruments de paiement", *JCP E.* 2010, 1034, 42; J. Sad, "Les services de paiement", in *Traité pratique de droit commercial – Tome 5: droit bancaire et financier*, Waterloo, Kluwer, 2016, 304.

[41] See for example: Ombudsfin 18 June 2019, nr. 2019.734; Ombudsfin 17 October 2017, nr. 2017.1173.

[42] Article 74.3 PSD2 and VII.44 §3 CEL.

to fulfil, either fraudulently or with intent or gross negligence the obligations imposed upon him by the law (in which case he is fully liable for all transactions before notification)[43].

Both PSD2 and the Belgian Code of Economic Law contain a few exceptions to this basic liability scheme. The payer cannot be held liable (except when the payer himself acted fraudulently) if 1) the PSP does not require strong customer authentication (*infra* nr. 23); 2) the PSP did not provide appropriate means for the notification at all times (*infra* nr. 18); 3) the loss, theft or misappropriation of the payment instrument was not detectable to the payer prior to a payment (*infra* nr. 26); and 4) the loss was caused by acts or lack of action of an employee, agent, or branch of a PSP or an entity to which its activities were outsourced. The Belgian Code of Economic law contains an additional exception: the payer cannot be held liable if he was not informed by the PSP of the measures he could take to keep the instrument safe, of the risks of liability or of the entity that must be notified in case of loss, theft or misappropriation of the instrument[44].

1. Turning Point: Notification

17. Since notification plays such an important role, it is no surprise that the PSD2, as well as Belgian law[45], contain some specific rules in this regard. Payers must notify loss, theft or misappropriation

[43] Article 74.1 PSD2 and article VII.44 §1 CEL.

[44] Article VII.189 CEL. PSUs can also find information on the "Wikifin"-website of the Financial Services Market Authority (FSMA) which is responsible in Belgium for the education of financial consumers : https://www.wikifin.be/fr/thematiques/votre-argent-au-quotidien/en-toute-securite/comment-payer-en-toute-securite and https://www.wikifin.be/fr/thematiques/votre-argent-au-quotidien/moyens-de-paiement/carte-de-credit-volee-ou-perdue-que-faire. The existence of this website cannot exempt the PSP from his information obligation towards the payer.

[45] Article VII.38 and VII.39 CEL.

of the instrument without undue delay on becoming aware of it[46]. When exactly someone becomes aware of loss, theft or unauthorized use of the instrument might be hard to determine. Therefore, it might be necessary to objectify this moment, implying that the obligation to notify the PSP originates when one is or *should have been* aware of the unauthorized use of the instrument[47]. However, in this context it is important to stress that there is no obligation to verify every day whether unauthorized transactions have taken place, nor whether one is still in possession of all his or her payment instruments[48]. The circumstances of the case, and in particular how often one uses the lost or stolen instrument (or the account on which the unauthorized transactions were registered), will be important in this context[49].

18. PSPs must make it possible for the payer to notify unauthorized use of a payment instrument 24/7[50]. The violation of this obligation is sanctioned severely, since PSPs cannot hold the payer liable when they did not provide appropriate means for notification at all times[51]. It seems that no causal link is required between the violation of this obligation and the unauthorized transactions that have taken place in order for this sanction to apply.

If PSPs employ third entities for notification purposes, they will be fully liable for mistakes made by these entities. In Belgium, it

---

[46] See for example: Ombudsfin 20 June 2017, nr. 2017.802; Ombudsfin 21 February 2006, nr. 2005/1084, considering notification taking place after eight or three hours, too late. See also: A. Van Oevelen, "De adviespraktijk van het Ombudsfin betreffende de aansprakelijkheid bij verlies of diefstal van elektronische betaalinstrumenten", *BFR* 2010, 298. Loss or theft of a mobile phone might require several notifications if several payment apps are installed on it.

[47] T. Baes, *ibidem*, 165.

[48] Court of Appeal Brussel 4 October 2005, *Revue du droit bancaire et financier* 2006, 148 ; Ombudsfin 24 August 2004, nr. 2004.850.

[49] Y. Gérard, *ibidem*, 42.

[50] Article VII.39, 3° CEL; W. Vandevoorde, "De Belgische wetgeving tot omzetting van Richtlijn 2007/64/EG betreffende betalingsdiensten in de interne markt. Een overzicht", *Tijdschrift voor Financieel Recht* 2011, 27.

[51] Article VII. 189 CEL.

was also decided that PSPs must ensure that these third entities are provided with all the information they need in order to block a stolen instrument. The decision was made in a case where a man and woman had several payment instruments, connected to different payment accounts and in which the wrong payment instrument was blocked because the third entity was not informed by the PSP that the payment instrument was connected to two different accounts[52].

19. Once notification has taken place, the PSP must prevent further use of the instrument[53]. In Belgium, Ombudsfin had to answer (indirectly) the question which details need to be communicated at the time of notification in a case where unauthorized transactions had taken place between a first notification during which a card holder could only mention his identity and a second notification where he was able to communicate his card / account number. Ombudsfin decided that PSPs must ensure that the blocking of the instrument is possible as soon as the payer provides his identity, since not all payers will be able to communicate their account number or the number of their payment instrument, when the instrument is lost or stolen[54].

2. Unauthorized transactions before notification

a. Basic liability rule

20. As already mentioned, the payer's liability is limited up to 50 euro[55], unless when he failed to fulfil, either fraudulently or with

---

[52] Commercial court Mons 28 April 2011, *Revue du Droit Commercial* 2013, 598.

[53] Art. VII.39,5° CEL; Ombudsfin, 17 January 2012, nr. 2011.1693; I. De Poorter, *ibidem*, 1342; J. Sad, *ibidem*, 310 ; M.-D. Weinberger, "Tendances de la médiation bancaire et financière en 2012", *Revue du droit bancaire et financier* 2013, 204.

[54] Ombudsfin 21 February 2006, nr. 2005.1084.

[55] The limitation of liability applies per payment instrument. Therefore the loss or theft of a mobile phone on which several payment apps were installed, can lead to a liability exceeding 50 euro (even if the payer did not act grossly negligent).

intent or gross negligence the obligations imposed upon him by the law[56]. As PSD2, the Belgian Code of Economic Law does not define the concept of gross negligence. A mere breach of the duty of care is not sufficient to conclude to the existence of gross negligence[57].

21. Article VII.44 §4 CEL however contains a few examples of behaviour that constitutes gross negligence. It determines that, amongst other things, must be considered as gross negligence: 1) writing down the PIN in an easily recognizable form, in particular on the payment instrument or a document that is kept together with the instrument[58] and 2) not informing the PSP immediately after becoming aware of loss, theft or unauthorized use of the instrument. It is remarkable that the Belgian legislator seems to indicate that a late notification automatically constitutes gross negligence. In any case, it is clear that article VII.44 §4 CEL just provides a few examples. Other behaviour, implying that the payer acts in breach of the terms governing the use of the instrument and in particular the obligation to keep the personalized security credentials safe, might also constitute gross negligence[59].

The latter is also shown by court decisions and decisions of Ombudsfin. For example, it was decided that a payer acts grossly negligent when he leaves his instrument in a place which is accessible to third persons (such as a hotel room, a hospital room or

---

For example, if three apps were installed and all of them have been used without authorization, the payer will be liable for 150 euro (50 euro for every payment instrument).

[56] Article 74.1 PSD2 and article VII.44 §1 CEL. There needs to be a causal link between the payer's gross negligence and the unauthorized transactions: T. Baes, *ibidem*, 182.

[57] Court of Appeal Brussels 4 October 2005, *Revue du droit bancaire et financier* 2006, 148 ; Ombudsfin 20 June 2017, nr. 2017.802; Ombudsfin 24 August 2004, nr. 2004.850; Ombudsfin 16 April 2013, nr.2012.2580.

[58] See also recital nr. 72 PSD2; M.-D. Weinberger (2013), *ibidem*, 165. Writing down the PIN or password on another document is not automatically considered gross negligence: T. Baes, *ibidem*, 180-181.

[59] J. Sad, *ibidem*, 306.

a train's luggage department)[60], as well as when he keys in his PIN, while he notices (or should have noticed) that he is being watched[61]. However, payers are not considered grossly negligent when they are spied on when keying in the PIN (without being aware of it)[62], neither when they secure their instrument with a simple PIN (e.g. 1234, birthday)[63] or several instruments with the same PIN[64].

22. Equally important is the question who bears the burden of proof. Article VII.44 §4 CEL imposes the burden of proof on the PSP. The mere registration of the use of the instrument and its personalized security credentials are not sufficient in order to prove (gross) negligence on behalf of the payer. Therefore, PSPs will need to provide supporting evidence to prove gross negligence[65]. In case of doubt, the PSP will bear the losses of unauthorized payment transactions (except for 50 euro)[66].

Although the Code of Economic Law does not accept the application of a so-called presumption of gross negligence, other presumptions are occasionally accepted by Ombudsfin. For example, Ombudsfin already concluded to gross negligence if the circumstances make it clear that there is no other plausible explanation for the unauthorized transactions

---

[60] Court of Appeal Brussels 23 June 2011, *Droit de la Consommation* 2012/95, 120; Cantonal Court Brussels 7 July 2006, *Revue du droit bancaire et financier* 2007, 134 ; Ombudsfin 15 January 2013, nr. 2012.1827 ; Y. Gerard, *ibidem*, 42.

[61] Ombudsfin 20 June 2017, nr; 2017.802; Ombudsfin 19 May 2015, nr. 2015.348; Ombudsfin 20 February 2019, nr. 2018.4161, where the payer introduced his PIN on demand of a third person.

[62] Commercial court Mons 28 April 2011, *Revue du Droit Commercial* 2013, 598.

[63] Ombudsfin 19 May 2015, nr. 2015.348; Ombudsfin 20 June 2015, nr.2016.3121; M.-D. Weinberger (2013), *ibidem*, 203.

[64] Ombudsfin 15 januari 2013, nr. 2012.1827; M.-D. Weinberger (2013), *ibidem*, 203.

[65] Ombudsfin 20 March 2018, nr. 2018.159.

[66] Ombudsfin 9 October 2018, nr. 2018.2037; M.-D. Weinberger, "Tendances de la médiation bancaire et financière en 2011", *Revue du droit bancaire et financier* 2012, 165.

than the payer's gross negligence[67]. More specifically, time and place play an important role in this context. Suppose that a payment card is lost or stolen in a foreign country, where the card holder spends his holiday but did not use the payment instrument. If the fraudster was able to key in the correct PIN immediately, the only plausible explanation is that the PIN has been written on the instrument or a document kept together with the instrument. Indeed it is impossible (or at least very unlikely) that the fraudster has been able in such a situation to spy on the PIN or detect the PIN on the basis of the instrument itself.

b. Transactions without strong customer authentication

23. The payer will not bear any financial consequences for unauthorized payment transactions if the PSP did not require strong customer authentication, except where the payer himself acted fraudulently[68]. Strong customer authentication is an authentication that is based on the use of *at least* two elements (so called two factor authentication) categorized as *knowledge* (something only the user knows, such as a PIN or a password), *possession* (something only the user possesses, such as a payment card or a token) and *inherence* (something the user is, such as a fingerprint, scan of the iris or voice recognition)[69]. For example, payment transactions on the Internet taking place through the mere communication of the credit card details (card number, expiry date and verification code) do not require *strong* customer authentication. The same goes for payments that can be initiated through a mobile phone or with a payment card, without a PIN, password or any biometrical data (e.g. use of NFC not requiring a PIN).

---

[67] Ombudsfin 18 December 2018, nr. 2018.2910; Ombudsfin 22 August 2006, nr. 2006.0660.

[68] Article 74.2 PSD2 and VII.44 §2 CEL.

[69] These elements must be independent, so that the breach of one does not compromise the reliability of the others.

24. It is of utmost importance to understand that this exemption from liability does not only apply where the PSP had to provide for strong customer authentication[70], but also when the PSP is exempted from strong customer authentication by the regulatory technical standards developed by EBA[71]. Therefore, PSPs must understand that when they choose not to apply strong customer authentication, this might have an important impact on their civil liability *towards the payer*, since, in their relation to the payer, they will be liable for all unauthorized transactions, not requiring strong customer authentication[72].

25. In Belgium, the introduction of the new rule making it impossible to hold the payer liable in the absence of strong customer authentication, led to the abolition of another rule that existed since 2002 and which, at least in some cases, led to the same result[73]. More specifically, this rule determined that payers could

---

[70] See 97 PSD2.

[71] Following the EBA opinion of 16 October 2019 on the deadline and process for completing the migration to strong customer authentication (SCA) for e-commerce card-based payment transactions (https://eba.europa.eu/eba-publishes-opinion-on-the-deadline-and-process-for-completing-the-migration-to-strong-customer-authentication-sca-for-e-commerce-card-based-payment) the National Bank of Belgium (NBB) reiterated that the legal deadline for complying with the RTS and the SCA requirements remains 14 September 2019, but it also acknowledged the challenges thereof in relation to e-commerce transactions. Therefore, the NBB indicated that it will cooperate with industry stakeholders to agree on a reasonable and acceptable plan for migrating the industry to SCA implementation for card payments as soon as possible after 14 September 2019 (https://www.nbb.be/doc/cp/eng/2019/20190828_nbb_2019_23.pdf). The latter has however no impact on the rules on the allocation of liability: Explanatory Memorandum, Chamber of Representatives, Doc. 54, 3131/001, 48.

[72] However, this does not mean that it will be the payer's PSP that will eventually bear the financial losses. If the payee or the payee's PSP fails to accept strong customer authentication, they will have to refund the financial damage caused to the payer's PSP (art. 74.2 PSD2 and article VII.44 §2 CEL).

[73] P. Berger, I. Van Biesen & S. Liebaert, "De impact van de nieuwe richtlijn betalingsdiensten (PSDII) op de Europese betaalmarkt", *TBH* 2017,131; J. Sad, *ibidem*, 310.

not be held liable in case unauthorized payment transactions took place *without physical presentation and electronic identification of the instrument*[74]. If for example an unauthorized payment transaction over the Internet took place by the mere provision of credit card details, the payer could not be held liable (since the instrument was not presented physically, nor identified electronically). However, the new rule, requiring strong customer authentication applies in more situations than the old one, and therefore offers additional protection. For example, payments in a shop with a payment card, not requiring a PIN, did not fall under the old exception (since there was physical presentation of the instrument) but do fall under the new exception (since there is no strong customer authentication).

c. Transactions not detectable to the payer prior to payment

26. Finally, it is important to stress that the payer cannot be held liable for unauthorized payment transactions, when the loss, theft or misappropriation of the payment instrument was not detectable to the payer prior to the payment[75]. Obviously, this is the case when a payment system or instrument has been hacked. Furthermore, the question arises whether the victim of *phishing, vishing or smishing* – where scammers convince the payer to communicate personalized payment credentials, either on a website or over the phone, in order to initiate unauthorized payment transactions or to install payment apps – could escape from liability for unauthorized transactions on the basis of this provision[76]. Answering this question, the wording of article VII.44 §1 CEL is very important. Decisive is not whether the payer involved actually *detected* the fraud, but whether it was

[74] See for example: Court of Appeal Brussel 19 April 2013, *Revue de Droit Commercial* 2015, 185; Court of Appeal Brussels 18 June 2007, *Nieuw Juridisch Weekblad* 2007, 935.

[75] Article VII.44 §1 CEL.

[76] P. Berger, I. Van Biesen & S. Liebaert, *ibidem*, 133.

detectable to the payer[77]. Therefore, the payer will only escape liability if a normal, reasonable and prudent payer would not have detected the fraud, taking into account the circumstances of the case[78]. If the fraud is detectable, it is very likely that the payer's behavior also constitutes gross negligence.

27. Before the transposition of PSD2, the Belgian CEL contained another rule, determining that the payer could not be held liable when transactions took place on the basis of a counterfeited instrument, or when the payer was still in possession of the payment instrument at the time the unauthorized transactions took place[79]. The latter provision offered more protection than the new one. For example, the payer could not be held liable in case scammers obtained information from the payer that was necessary to install the PSP's payment app. Indeed, in such situation the payer was still in possession of his payment instrument. According to the new rule, it will depend on the circumstances whether the payer can be held liable. Only if the fraud was not detectable to the payer, he will escape liability.

d. Faults of PSPs

28. The question was raised whether faults or carelessness of a PSP can have an impact on the allocation of liability. The following case illustrates the importance of the question. A payer was contacted by phone after advertising a second hand good on an online market place. The scammer asked the payer not to communicate PIN or password, but to communicate the code that is generated using the Digipass and PIN (*vishing*). According to the scammer this was

[77] No reference is made as to the burden of establishing detectability : M. Donnelly, "Payments in the digital market: Evaluating the contribution of Payment Services Directive II", *Computer Law & Security Review* 2016, 835.

[78] Ombudsfin 18 June 2019, nr. 2019.734.

[79] Ombudsfin 18 December 2018, nr. 2018.1847.

necessary in order to allow payment to the payer. The scammer, claiming that an error occurred, was able to convince the payer to communicate the code 16 times. An amount of 4,020 euro (16 times 251 or 252.50 euro) was debited from the payer's account in a few minutes. Ombudsfin decided the payer was fully liable, since the payer acted grossly negligent[80].

Although it is clear that a normal and prudent payer should have detected the fraud prior to the unauthorized transactions taking place and communicating the code 16 times must be considered gross negligence, it can be argued that the PSP was also negligent. PSPs must employ systems that enable them to detect and stop suspicious transactions (such as several transactions for the same or similar amount within a few minutes, moreover not being consistent with the payer's spending pattern). In such situation, where both the payer and the PSP have been negligent, liability should at least be divided upon the parties.

V. Conclusion

29. Whereas PSD2 increases consumer protection (in comparison with PSD1)[81], its transposition in Belgium has had a more modest impact. This is due to the fact that the Belgian legislator in 2009, when transposing PSD1, made use of the possibility of offering additional protection in case of unauthorized payment transactions. When transposing PSD2, the Belgian legislator decided to stick to the Directive's text and estimated that additional protection was no longer necessary (due to the higher level of protection offered by PSD2). Nevertheless, there might be cases where Belgian payers were better protected before the transposition of PSD2 (in particular in the context of phishing).

One of the most important findings relating to Belgian law is that it explicitly imposes the burden of proof with regard to the

[80] Ombudsfin, nr. 2019.3002 (not published).

[81] R. Steennot, *ibidem*, 963-964.

existence of gross negligence on the PSP. Therefore, Belgian law avoids that payers are being held liable without any limitation for all unauthorized transactions taking place before notification if they did not act grossly negligent. Moreover, the concept of gross negligence is generally interpreted restrictively by the courts, as well as by Ombudsfin. Unfortunately, Ombudsfin does not seem to take into account the PSP's fault or carelessness, once the payer's gross negligence has been established. Therefore, it is advised to the Belgian legislator to determine explicitly in article VII.44 CEL that the security measures taken by the PSP are to be taken into account when allocating liability.

Bibliography

A. Van Oevelen, De adviespraktijk van het Ombudsfin betreffende de aansprakelijkheid bij verlies of diefstal van elektronische betaalinstrumenten, BFR, 2010, no 5, pp. 294-305.

I. De Poorter, De wet betreffende de betalingsdiensten leidt tot een betere bescherming van de consument, RW, 2011, no 32, pp. 1330-1344.

J. Sad, Les services de paiement, in Traité pratique de droit commercial – Tome 5: droit bancaire et financier, Kluwer, 2016, Waterloo.

M. Donnelly, Payments in the digital market: Evaluating the contribution of Payment Services Directive II, Computer Law & Security Review, 2016, vol 32, no 6, pp. 827-839.

M.-D. Weinberger, Tendances de la médiation bancaire et financière en 2011, Revue du droit bancaire et financier, 2012, no. 3, pp. 164-175.

M.-D. Weinberger, Tendances de la médiation bancaire et financière en 2012, Revue du droit bancaire et financier, 2013, no. 4, pp. 202-216.

P. Berger & S. Landuyt, Toepassingsgebied van de wet betalingsdiensten en de wet betalingsinstellingen (in Financiële regulering in de kering), Intersentia, 2012, Antwerp.

P. Berger, I. Van Biesen & S. Liebaert, De impact van de nieuwe richtlijn betalingsdiensten (PSDII) op de Europese betaalmarkt, TBH, 2017, no 2, pp. 123 – 235.

R. Steennot & J. Goetghebuer, Bescherming van de consument bij niet-toegestane mobiele betalingstransacties (in Digitalisering van het recht en consumentenbescherming), Intersentia, 2019, Antwerp.

R. Steennot, Allocation of liability in case of fraudulent use of an electronic payment instrument: the new directive on payment services in the internal market, Computer Law & Security Review, 2008, vol 24, no 6, pp. 555 – 561.

T. Baes, "Aansprakelijkheid bij uitvoeringsincidenten in het betalingsverkeer", in IFR (ed.), *Financiële Regulering in de kering*, Antwerpen, Intersentia, 2012, 157-216.

W. Vandevoorde, De Belgische wetgeving tot omzetting van Richtlijn 2007/64/EG betreffende betalingsdiensten in de interne markt. Een overzicht, Tijdschrift voor Financieel Recht, 2011, no 3, pp. 2-85.

Y. Gérard, L'utilisation frauduleuse des instruments de paiement, JCP E., 2010, pp. 42.

Martin Miernicki[1]
(University of Vienna)

TRANSPOSITION OF THE PSD2 IN AUSTRIA

1. Introduction

The purpose of this contribution is twofold: First, it gives an overview of the transposition of the PSD2 and the relevant rules on payment services in Austria; second, it presents two special developments in the ambit of payment services that might be of interest for lawyers from other member states.

2. General remarks

2.1. Transposition of the PSD2 and the ZaDiG 2018

The general approach taken in the transposition process was to closely mirror the language and the structure of European rules.[2] Accordingly, the regulatory provisions and the rules on the relation between payment service providers (PSPs) and payment service users under private law are transposed through one comprehensive act. The PSD 1 was transposed in the Payment Services Act of 2009

[1] University Assistant (post doc), Department of Business Law.

[2] ErläutRV 207 BlgNR 24. GP 4, *available at* https://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_00207/fname_159443.pdf (accessed 30 January 2020).

(Zahlungsdienstegesetz – ZaDiG 2009)[3]; the Austrian legislator decided not to amend the ZaDiG 2009 but to enact a new act in the course of the transposition of the PSD2: the Payment Services Act of 2018 (Zahlungsdienstegesetz 2018 – ZaDiG 2018).[4] Even more than its predecessor, the act follows the structure and the wording of the PSD2. Where there are no special rules in the ZaDiG 2018, the General Civil Code of 1811 (Allgemeines Bürgerliches Gesetzbuch – ABGB)[5] applies. This is a common legislative strategy in Austria; for instance, the greatest parts on consumer protection have never been included in the ABGB but are contained in specials laws, like the Consumer Protection Act of 1979 (Konsumentenschutzgesetz – KSchG)[6] or the Act on Distance and Off-Premises Contracts (Fern- und Auswärtsgeschäfte-Gesetz – FAGG).[7]

2.2. Timeline

The implementation deadline of the PSD I was 1 November 2009 (Art 94 PSD I) and the ZaDiG 2009 entered into force on the same day (§ 79 ZaDiG 2009). The PSD2 had to be implemented by the member states by 13 January 2018 (Art 115 PSD2). The first draft on the new ZaDiG 2018 was published by the Federal Minister of Finance on 20 October 2017,[8] followed by a public consultation. Subsequently, however, the adoption was slightly delayed; most parts of the ZaDiG 2018 entered into force on 1 June 2018 (§ 119(1) ZaDiG

[3] BGBl I 2009/66. Austrian laws can be accessed via the federal legal information system (https://www.ris.bka.gv.at).

[4] BGBl I 2018/17.

[5] JGS 1811/946.

[6] BGBl 1979/140.

[7] BGBl I 2014/33.

[8] ME ZaDiG 2018, 332/ME 25. GP, *available at* https://www.parlament.gv.at/PAKT/VHG/XXV/ME/ME_00332/imfname_672716.pdf (accessed 30 January 2020).

2018), resulting in a delayed implementation of the PSD2 for a period of about six months.

As for the provisions on the confirmation on the availability of funds, payment initiation service providers, account information services (§§ 59-61 ZaDiG 2018), and the rules on strong customer authentication (§ 87 ZaDiG 2018), the date for the entry into force was generally 14 September 2019 (§ 119(2) ZadiG 2018, Art 115(4) in connection with Art 98 PSD2), based on the entry into force of the regulatory technical standards adopted by the Commission in March 2018 (Art 38(2) Regulation 2018/389).[9]

In relation to the rules on strong customer authentication, however, the European Banking Authority decided to allow for a more lenient implementation schedule due to the technical problems in the E-Commerce sector, especially with regard to those actors who are not themselves payment service providers, such as e-merchants.[10] The EBA phrased the extension as an authorization for national competent authorities ("supervisory flexibility");[11] this authority is the Austrian Financial Market Authority (FMA). Based on this opinion, the FMA decided, on 19 August 2019, to extent the implementation deadline for strong customer authentication (two-factor authentication) for card payments made online to give payment service providers and merchants more time to migrate

[9] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, OJ 2018, L 69, 23-43.

[10] *EBA*, Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2, EB-Op-2019-06, *available at* https://eba.europa.eu/eba-publishes-an-opinion-on-the-elements-of-strong-customer-authentication-under-psd2 (accessed 30 January 2020).

[11] "CAs may decide to work with PSPs and relevant stakeholders […] to provide limited additional time to allow issuers to migrate to authentication approaches that are compliant with SCA […] and acquirers to migrate their merchants to solutions that support SCA".

to SCA-compliant authentication approaches.[12] In the wake of the EBA opinion published on 16 October 2019,[13] the FMA, in specifying its prior announcement, extended the deadline on 17 October 2019 until 31 December 2020.[14]

2.3. Institutions

The competent authority for the authorization and supervision of PSPs is the FMA.[15] The FMA is not only competent for the enforcement and implementation of the PSD2, but the banking, insurance and security sectors in general. In several contexts, it carries out its tasks in cooperation with the Austrian National Bank (OeNB).

3. Member state options

The PSD2 is based on the concept of full harmonization; however, the directive contains several provisions that allow national law-makers to deviate from its rules (Art 107 PSD2). The most important member state options that have or have not been exercised in Austria will be summarized in the following.

---

[12] *FMA*, FMA extends implementation period for strong customer authentication for card payments in e-commerce, https://www.fma.gv.at/en/fma-extends-implementation-period-for-strong-customer-authentication-for-card-payments-in-e-commerce/ (accessed 30 January 2020).

[13] *EBA*, Opinion of the European Banking Authority on the deadline for the migration to SCA for e-commerce card-based payment transactions EBA-Op-2019-11, *available at* https://eba.europa.eu/eba-publishes-opinion-on-the-deadline-and-process-for-completing-the-migration-to-strong-customer-authentication-sca-for-e-commerce-card-based-payment (accessed 30 January 2020).

[14] *FMA*, FMA extends deadline for application of strong customer authentication for card payments in e-commerce transactions to 31.12.2020, https://www.fma.gv.at/en/fma-extends-deadline-for-application-of-strong-customer-authentication-for-card-payments-in-e-commerce-transactions-to-31-12-2020/ (accessed 30 January 2020).

[15] General rules on the operation and the internal structure of the FMA are contained in the Finanzmarktaufsichtsbehördengesetz – FMABG BGBl I 2001/97.

3.1. Surcharging

Based on Art 62(5) PSD2, the second sentence of § 56(3) ZaDiG 2018 specifies that payees may not request charges for the use of a specific payment instrument.[16] Thus, the provision contains a general prohibition from applying a surcharge in relation to the use of a specific payment instrument. Since the member state option of Art 62(5) PSD2 was fully exercised, a separate transposition of Art 62(4) was not necessary;[17] this is because Art 62(4) only refers to charges requested by the payee for the use of those payments instruments to which the regulation on interchange fees or those payment services to which the SEPA-Regulation apply, while Austria, based on the authorization in Art 62(5), decided to prohibit charges for specific payment instruments in general. For this reason, it was, furthermore, not necessary to separately transpose Art 19 Directive 2011/83/EU (Consumer Rights Directive)[18] that prohibits traders from charging consumers fees for the "use of a given means of payment" that "exceed the cost borne by the trader for the use of such means".[19] The general prohibition of surcharging had already been implemented prior to the PSD2 in § 27(6) ZaDiG 2009 (based on Art 52(3) PDS 1).[20] At the same time – and in compliance with the mandatory provision

[16] The original text reads: "Die Erhebung von Entgelten durch den Zahlungsempfänger im Falle der Nutzung eines bestimmten Zahlungsinstrumentes ist unzulässig." See on the background of the provision Weilinger/Knauder in Weilinger (ed.), ZaDiG (2017 update) § 27 at 21 et seq.

[17] ErläutRV 11 BlgNR 26. GP 16, *available at* https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00011/fname_679296.pdf (accessed 30 January 2020).

[18] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, OJ 2011, L 304, 64-88.

[19] ErläutRV 89 BlgNR 25. GP 7, *available at* https://www.parlament.gv.at/PAKT/VHG/XXV/I/I_00089/fname_343429.pdf (accessed 30 January 2020).

[20] ErläutRV 207 BlgNR 24. GP 34; ErläutRV 11 BlgNR 26. GP 16; *see* on this provision ECJ 9. 4. 2014, C-616/11.

of Art 62(3) PSD2 – the first sentence of § 56(3) ZaDiG 2018 permits payees to provide for incentives (*e.g.*, discounts) for the use of certain payment instruments and PSPs may not prevent payees from doing so.

3.2. Payer's liability for unauthorized payment transactions

The last subparagraph of Article 74(1) PSD2 allows member states to reduce the payer's liability in case of losses resulting from unauthorized payment transactions. This option was exercised in § 68(4) ZaDiG 2018.[21] This rule provides that, under certain circumstances, the PSP must bear parts of the losses ("Schadensteilung") in cases where the payer has neither acted fraudulently nor intentionally failed to fulfill its obligations under Art 69 PSD2 (§ 63 ZaDiG 2018). In order to determine the respective liability of the payer and the PSP, the nature of the personalized security credentials and the specific circumstances under which the payment instrument was lost, stolen or misappropriated must be taken into account. Additionally, § 68(1) ZaDiG 2018 confines the liability of the payer (referred to in the first sentence of Art 74(1) PSD2 – maximum threshold of 50 EUR) to cases where he or she acted with slight negligence.[22]

3.3. Derogations for low value payment instruments and Electronic money

Low value payment instruments receive special treatment compared to other payment instruments. Art 42 and 63 PSD2 provide for derogations from the rules contained in title III and title IV of the directive; for the purpose of both articles, a low value payment instrument is a framework-contract-based payment instrument that "concern only individual

[21] ErläutRV 11 BlgNR 26. GP 19.

[22] *See Koch*, Prüfung und Bearbeitung eines Überweisungsauftrags durch den beauftragten Zahlungsdienstleister nach ZaDiG 2018/PSD II, Österreichisches Bankarchiv 2019, 106 (111).

payment transactions that do not exceed 30 EUR or that either have a spending limit of 150 EUR or store funds that do not exceed 150 EUR at any time" (Art 42(1), *cf.* Art 63(1) PSD2).[23] Art 42(2) and 63(2) PSD2 permit the member states or their competent authorities to alter these amounts in respect of national payment transactions and Austria has done so in § 35(5) and § 57(2) ZaDiG 2018.[24] Accordingly, the relevant amounts for such transactions are set at 60 EUR concerning individual payment transactions, 300 EUR in relation to spending limits and 400 EUR with regard to prepaid instruments. As regards Electronic money (Art 63(3) PSD2), the ZaDiG 2018 introduces a threshold value of 400 EUR (§ 57(3) ZaDiG 2018).

3.4. Alternative dispute resolution

Based on Art 61(2) PSD2, Austria decided to confine the alternative dispute resolution measures set forth in Art 102 PSD2 to payment service users that are consumers.[25] Accordingly, the platform referred to in § 98 ZaDiG 2018 is not competent to deal with disputes arising between PSPs and non-consumers. This platform is called the Common Dispute Resolution Body of the Austrian Banking Industry (Gemeinsame Schlichtungsstelle der Österreichischen Kreditwirtschaft) which was founded by the Austrian Chamber of Commerce.[26]

3.5.Microenterprises and small payment institutions

The ZaDiG 2018 does not exercise the option contained in Art 38(2) and Art 61(3) to extend the protection for consumers under Title III and Title IV to microenterprises (Art 4(36) PSD2).[27] In a similar

[23] The definitions are practically identical.

[24] ErläutRV 11 BlgNR 26. GP 17.

[25] ErläutRV 11 BlgNR 26. GP 23 f.

[26] https://www.bankenschlichtung.at/ (accessed 30 January 2020).

[27] ErläutRV 11 BlgNR 26. GP 13, 16.

fashion, the Austrian legislator refrained from introducing exceptions from the rules on authorization and supervision with regard to "small payment institutions" (Art 32 PSD2). However, § 23a FMABG (that was introduced in 2020) provides for a "regulatory sandbox". The aim of the provision is to foster innovative business models.

4. Data protection

Data protection and privacy laws become more and more relevant in the area of payment services. This development is also connected to the entry into force of the GDPR.[28] The relationship between the GDPR and the PSD2 is, however, not always free of tensions.

4.1. The transposition of Art 94 PSD2

The PSD2 addresses data protection in Art 94. The general rule set forth by this provision is that "payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user" (Art 94(2) PSD2). For reasons that are not entirely clear, the Austrian legislator chose to transpose this rule in two separate provisions – § 24 and § 90 ZaDiG 2018. While § 90 contains, following the structure of the PSD2, the general rule on the protection of personal data, § 24 refers – based on Art 21 PSD2 – to record keeping; the latter article does not explicitly mention the protection personal data.[29] Admittedly, § 24 ZaDiG 2018 and Art 21 PSD2 do concern the protection of

[28] 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, OJ 2016, L 119, 1-88.

[29] "Member States shall require payment institutions to keep all appropriate records for the purpose of this Title for at least 5 years, without prejudice to Directive (EU) 2015/849 or other relevant Union law."

personal data in a wider sense because the recording and the storage of personal data constitute acts of "processing" within the meaning of Art 4(2) GDPR. However, it remains obscure why the Austria legislator deemed a transposition of Art 94 PSD2 (only) in § 90 ZaDiG 2018 insufficient. In fact, the foundations of the current legal situation had already been laid in § 18 and § 61 ZaDiG 2009, against the background of a similar European legal basis (Art 79 PSD I). Moreover, § 24 and § 90 ZaDiG 2018 use a different wording: While § 24 ZaDiG 2018 refers to "ausdrückliche Einwilligung",[30] § 90(4) ZaDiG 2018 speaks of "ausdrückliche Zustimmung".[31] Both versions can be translated to English as "explicit consent" but do constitute different terms in German; the latter term might, in certain situations, be understood to refer to a contractual relation under private law rather than to a consent given within the meaning of the laws on data protection.[32] However, there is no indication that the Austrian legislator desired to implement a different meaning in the two related sections. The current wording of the ZaDiG 2018 might be the result of the rather complicated legislative history of the two provisions, as the rules on data protection were moved back and forth between § 24 and § 90 in different versions in the course of the transposition of the GPDR and the PSD2 and were also altered in comparison to the respective drafts.

It should be noted that it is not clear whether Art 94 PSD2 and §§ 24, 90 ZaDiG 2018 refer to an explicit consent within the meaning of the GDPR[33] or an explicit contractual consent under the rules of

---

[30] "Zahlungsdienstleister dürfen die für das Erbringen ihrer Zahlungsdienste notwendigen personenbezogenen Daten nur mit der ausdrücklichen Einwilligung des Zahlungsdienstnutzers verarbeiten."

[31] "Zahlungsdienstleister dürfen die für das Erbringen ihrer Zahlungsdienste notwendigen personenbezogenen Daten nur mit der ausdrücklichen Zustimmung des Zahlungsdienstnutzers abrufen, verarbeiten und speichern."

[32] *Cf. Duy/Stempkowski*, PSD II und Datenschutz, Österreichisches Bankarchiv 2018, 791 (794-795).

[33] There, the term "consent" of the data subject refers to "any freely given, specific, informed and unambiguous indication of the data subject's wishes by

the regime for payment services. The prevailing opinion in Austria – given the practical problems and the inherent inconsistencies with other sectors where an explicit consent under the GDPR is not required – seems to be that Art 94 and the corresponding provisions in the ZaDiG 2018 are not to be construed as a reference to the GPDR but rather to a reference to contractual principles for the provision of payment services.[34] This approach seems to be reasonable; furthermore, the opinion of the European Data Protection Board appears to be of the same opinion.[35]

4.2. Case law on the relationship of payment services and the protection of personal data

Recent case law analyzed the relationship of PSPs and payment service users from the perspective of both the PSD2 and the GDPR.

The facts of the first case[36] were the following: Due to a dispute, a person requested – free of charge – account statements in respect of the last five years from her PSP;[37] online access was provided, but only with regard to the past year. The PSP was, in principle, willing to issue the statements but demanded a payment of 120 EUR (= 30 EUR year for each of the four years, 2013-2016). As far as can be seen, this was in conformity with the laws on payment services as well

---

which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (Art 4(11) GPDR). While under Art 6 GDPR, the data subject's consent need not necessarily be "explicit", Art 9(2)(a) GDPR requires – in respect of special categories of personal data – an "explicit" consent.

[34] *See*, *e.g.*, *Duy/Stempkowski*, Österreichisches Bankarchiv 2018, 791 (795).

[35] *European Data Protection Board*, Letter EDPB-84-2018, https://edpb.europa.eu/sites/edpb/files/files/file1/psd2_letter_en.pdf (accessed 30 January 2020).

[36] *See* BVwG 24.5.2019, W258 2205602-1; the court already applied the GDPR and the ZaDiG 2018.

[37] To be specific, the request referred to transaction data concerning the building administration.

as the corresponding framework contract; however, the claim was not based on these rules but rather on the right of access to personal data (which is now regulated in Art 15 GDPR). Since the PSP did not comply with the request, a complaint was filed with the Austrian Data Protection Authority (DSB).[38] The DSB found the complaint to be substantiated; later, the decision was upheld by the Federal Administrative Court (Bundesverwaltungsgericht – BVwG).

In essence, the question was whether the rules of the ZaDiG 2018 would prevail over the rules of the GDPR. The court held that the rules of the PSD2 were, compared to Art 15 GDPR, of a different nature; while Art 15 GPDR refers to a *right of access*, based purely on the data subject's initiative, the rules for payment services were interpreted as *information obligations*, obliging the PSP to take actions to inform the payment service user.[39] Moreover, the court did not consider the request to be "manifestly unfounded or excessive" within the meaning of Art 12(5) GDPR which states that the information under Art 15 GDPR shall be provided free of charge; the court explicitly ruled that it did not matter that the information request under the GDPR was only made to circumvent the fees that would have been due according to the rules of the ZaDiG 2018 and framework contract.[40] Accordingly, the BVwG held that the rules of the PSD2 and the ZaDiG 2018 were not *leges speciales* in relation to the GDPR and the complainant could indeed rely on the framework of data protection to enforce her rights; both types of rights essentially exist in parallel. It is not surprising, that there exist diverging views on this question in Austria.[41] Indeed, one could

---

[38] DSB 21. 6. 2018, DSB-D122.844/0006-DSB/2018.

[39] BVwG 24.5.2019, W258 2205602-1 at 3.4.3.1.-3.4.3.7. referencing ECJ 7. 5. 2009, C-553/07 at 69; the BVwG explicitly considered it to be irrelevant that the obligations under § 53(2) ZaDiG 2018 (and Art 57(2) PSD2) are trigged upon the payer's request.

[40] BVwG 24.5.2019, W258 2205602-1 at 3.4.4.1.-3.4.4.5.

[41] *See*, *e.g.*, *Knoll*, Kontodaten nach der DSGVO, Datenschutz konkret 2019, 32 (33) (considering the ZaDiG 2018 as a *lex specialis*); *see also Koch*, ÖBA 2019, 106 (114-115).

ask whether the court's reliance on the cited decision of the ECJ requires further analysis. This is because the ECJ delivered its opinion on the relation between different provisions of the same directive, whereas the GDPR and the PSD2 constitute two separate acts of legislation that are not necessarily fully coherent from a systematical point of view.

A different case before the BVwG[42] that also involved the data protection laws concerned a claim for information in written form regarding, amongst others, the account movements of the complainant's account in the course of the preceding seven years. The court acknowledged that payment documents can contain personal data not only of the concerned person, but also of third parties (*cf.* Art 15(4) GDPR); and that the right to access to data aims at enabling the data subject to examine whether the processing of the data was lawful. However, the court upheld the claim insofar as the claimant's personal data were concerned.[43]

5. Regulation of cash withdrawal services by means of ATM

5.1. Transposition of the exception for "independent ATM operators"

According to Art 3(o) PSD2, "cash withdrawal services offered by means of ATM by providers, acting on behalf of one or more card issuers, which are not a party to the framework contract with the customer withdrawing money from a payment account," do not fall within the scope of the PSD2, "on condition that those providers do not conduct other payment services as referred to in Annex I". A similar provision was contained in Art 3(o) PSD I. Accordingly, as long as these providers – which are also referred to as "independent ATM operators" – do not provide other payment services, the PSD2 does not apply to them and they are not considered as payment service providers. However, in the second sentence of Art 3(o), the PSD2 introduces new information requirements

[42] BVwG 10. 12. 2018, W211 2188383-1.

[43] BVwG 10. 12. 2018, W211 2188383-1 at 3.2.2.3.

for independent ATM operators; under the new rules, "the customer shall be provided with the information on any withdrawal charges referred to in Articles 45, 48, 49 and 59 before carrying out the withdrawal as well as on receipt of the cash at the end of the transaction after withdrawal." With regard to the new information obligations, the corresponding Austrian provision (§ 3(3)(15) ZaDiG 2018) employs a slightly different wording:

> *This act does not apply to*
> *[…]*
> *15. cash withdrawal services by means of multifunctional ATMs for one or more card issuers, offered by providers that have not concluded a framework contract with the customer who withdraws the cash from a payment account, on condition that*
> *· those providers do not conduct other payment services and*
> *· those providers provide the customer with information on any withdrawal charges in accordance with §§ 36, 41, 44, 45, both prior to the withdrawal as well as on receipt of the cash after withdrawal.*[44]

Accordingly, a strict reading of the provision would suggest that independent ATM operators can only benefit from the exception contained in § 3(3)(15) ZaDiG 2018 if they fulfill the new information obligations, as these obligations are worded as one of two necessary conditions in the Austrian transposition. However, this does not necessarily follow from Art 3(o) PSD2; rather, for the sake of transparency, the provision aims at declaring certain information obligations applicable with regard to cash withdrawal services that

[44] Translated and paraphrased by the author; the original text reads: "Dienste von Dienstleistern, die keinen Rahmenvertrag mit dem von einem Zahlungskonto Geld abhebenden Kunden geschlossen haben, bei denen für einen oder mehrere Kartenemittenten an multifunktionalen Bankautomaten Bargeld abgehoben wird, vorausgesetzt, dass

a) diese Dienstleister keine anderen der in § 1 Abs. 2 genannten Zahlungsdienste erbringen und

b) den Kunden alle Entgelte für Geldabhebungen gemäß den §§ 36, 41, 44 und 45 sowohl vor der Abhebung als auch auf der Quittung nach dem Erhalt von Bargeld mitgeteilt werden."

otherwise do not fall within the scope of the directive (recital 18 PSD2). Therefore, it appears that the information obligations are of a private law nature and do not constitute a separate requirement for the application of Art 3(o) PSD2. Thus, with regard to directive, the § 3(3)(15) ZaDiG 2018 should be interpreted accordingly.

5.2. Regulation of ATM fees

Traditionally, Austrian banking institutions have formed a network for the provision of cash withdrawal services by means of ATM. As a result of this collaboration, fees for cash withdrawals at Austrian ATMs with debit cards in connection with Austrian payment accounts were rather uncommon. However, in recent years, ATM operators which were not part of the common ATM network entered the Austrian market, charging a fee for their cash withdrawal services.[45] Against this background, § 4a was added[46] to the Consumer Payment Account Act (Verbraucherzahlungskontogesetz – VZKG) that entered into force on January 13, 2018 (and thus prior to the entry into force of the ZaDiG 2018). The VZKG's main purpose is to transpose the Payment Accounts Directive[47] into Austrian law; this choice was made by the Austrian legislator for systematic reasons.

The new provision stated:

---

[45] For more background information, *see, e.g.,* OGH 18. 12. 2017, 9 Ob 63/17 f; VfGH 9. 10. 2018, G 9/2018-24, G 10/2018-27; IA 2284/A 25. GP 2, *available at* https://www.parlament.gv.at/PAKT/VHG/XXV/A/A_02284/imfname_669976.pdf; *Bundeswettbewerbsbehörde*, Stellungnahme zur Regulierung von Bankomatgebühren, BWB/AW-412 (2017), *available at* https://www.bwb.gv.at/fileadmin/user_upload/News/PDFs_News/BWB2016-re-Stellungnahme_Bankomatgebu__hren_ZUSAMMENFASSUNG.pdf.

[46] BGBl I 2017/158.

[47] Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features, OJ 2014, L 257, 214-246.

> *The payment service provider shall relieve the consumer from the payment of any charges that a provider under § 2(3)(15) ZaDiG requests for cash withdrawals that the consumer carries out by using a payment card issued for the payment account.*[48]

As can be seen, the purpose of the provision was that the consumer would not have to bear any costs for cash withdrawals and that the associated charges would be paid by her PSP. According to the legislative materials, the provision should ensure the access of the general public to cash, especially in sparsely populated areas.[49] Not surprisingly, however, the provision proved to be highly controversial. Most importantly, the question arose whether § 4a VZKG was compatible with the Austrian Constitution and eventually the provision was challenged before the Austrian Constitutional Court (VfGH). In October 2018, the court held the provision to be unconstitutional. The VfGH based its opinion on the fundamental right to property which is protected by Art 15 of the Basic Law on the General Rights of Nationals of 1867 (Staatsgrundgesetz 1867 – StGG 1867)[50] and Art 1 of the First Additional Protocol of the European Charta on Human Rights (which also forms a part of the Austrian Constitution). The argument that convinced the court was that it would be disproportional to require PSPs to bear costs that are beyond their control and that are agreed upon between the customer and the ATM operator without their participation; moreover, there was no maximum threshold provided for by § 4a VZKG.[51] As a result, there is no general obligation for PSPs to bear

---

[48] Translated and paraphrased by the author. The original text stated: "Der Zahlungsdienstleister hat den Verbraucher von der Zahlung von Entgelten zu befreien, die ein Dienstleister gemäß § 2 Abs. 3 Z 15 ZaDiG vom Verbraucher für Bargeldabhebungen mit der zum Zahlungskonto des Verbrauchers ausgegebenen Zahlungskarte beansprucht."

[49] IA 2284/A 25. GP 3.

[50] RGBl 1867/142.

[51] VfGH 9. 10. 2018, G 9/2018-24, G 10/2018-27 at IV.2.1.-2.5.3.

to the costs of cash withdrawals by means of ATMs; they can also, in principle, provide for their own fees in the framework contracts, provided that they comply with the provisions on consumer protection (especially § 4(2) VZKG).[52]

5.3. Contractual framework regarding ATM fees

Independent from the fact that § 4a VZKG was repealed by the VfGH, ATM fees have led to a string of cases before the Austrian Supreme Court (OGH). The question was whether PSPs were obliged to bear the fees charged by independent ATM operators for cash withdrawals on the basis of the framework contract concluded between the PSP and the customer. The OGH[53] answered the question in negative; according to the court, a customer concludes a contract with the independent ATM operator when using the cash withdrawal services at the ATM. This contract possesses characteristics of a contract on a single payment transaction within the meaning of Art 43 PSD2[54] and possible fees are due under this contract. Of course, the independent ATM operator has to inform the customer about the requested fees (Art 3(o) PSD2). In turn, the card issuing PSP is under no obligation regarding the fees charged by independent ATM operators. The duties stemming from the framework contracts as used in Austria are confined to enabling the customer to access her payment account via the terminals of independent ATM operators.[55]

---

[52] Contractual terms of this kind must be individually negotiated in order to be valid. The VfGH deemed this provision to be constitutional.

[53] OGH 14. 3. 2018, 10 Ob 14/18 h.

[54] However, strictly speaking, it is not such a contract because independent ATM operators are not PSPs under the PSD2, see *Faber*, Bankomatgebühren, Österreichisches Bankarchiv 2018, 164 (167).

[55] OGH 14. 3. 2018, 10 Ob 14/18 h at 1.3.4.

6. Conclusion

The PSD2 implies new challenges, especially in the field of third party providers and the relationship between the law of payment services and data protection. In parallel, the implementation of the rules on strong customer authentication has proven difficult. While the PSD2 has addressed important ambiguities, some interpretative problems (that will ultimately have to be resolved by the ECJ) remain; a recent example constitutes the ECJ's decision in DenizBank (C-287/19). Furthermore, it remains to be seen whether the concept of "open banking" will be further developed to broader concept of "open finance" that would also include a person's investments, for instance.

Legal Literature

J. Duy/P. Stempkowski, *PSD II und Datenschutz*, in *Österreichisches Bankarchiv*, 2018, pp. 791-796.

W. Faber, *Bankomatgebühren*, in *Österreichisches Bankarchiv*, 2018, pp. 164-184.

M. Knoll, *Kontodaten nach der DSGVO*, in *Datenschutz konkret*, 2019, pp. 32-34.

B. Koch, *Prüfung und Bearbeitung eines Überweisungsauftrags durch den beauftragten Zahlungsdienstleister nach ZaDiG 2018/PSD II***,** in *Österreichisches Bankarchiv***,** 2019, pp. 106-119.

G. Tuder, *Grundsatzfragen des ZaDiG infolge der ZDRL II*, finanzverlag, 2019, Vienna.

A. Weilinger (ed.), *ZaDiG*, Manz, updated 2017, Vienna.

Reports, Opinions and Press Releases

BUNDESWETTBEWERBSBEHÖRDE, Stellungnahme zur Regulierung von Bankomatgebühren, BWB/AW-412, 2017, *available at* https://www.bwb.gv.at/fileadmin/user_upload/News/PDFs_News/BWB2016-re-Stellungnahme_Bankomatgebu__hren_ZUSAMMENFASSUNG.pdf.

EUROPEAN BANKING AUTHORITY, Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2, EB-Op-2019-06, *available at* https://eba.europa.eu/eba-publishes-an-opinion-on-the-elements-of-strong-customer-authentication-under-psd2 (accessed 30 January 2020).

EUROPEAN BANKING AUTHORITY, Opinion of the European Banking Authority on the deadline for the migration to SCA for e-commerce card-based payment transactions, EBA-Op-2019-11, *available at* https://eba.europa.eu/eba-publishes-opinion-on-the-deadline-and-process-for-completing-the-migration-to-strong-customer-authentication-sca-for-e-commerce-card-based-payment (accessed 30 January 2020).

FINANCIAL MARKET AUTHORITY, FMA extends implementation period for strong customer authentication for card payments in e-commerce, https://www.fma.gv.at/en/fma-extends-implementation-period-for-strong-customer-authentication-for-card-payments-in-e-commerce/ (accessed 30 January 2020).

FINANCIAL MARKET AUTHORITY, FMA extends deadline for application of strong customer authentication for card payments in e-commerce transactions to 31.12.2020, https://www.fma.gv.at/en/fma-extends-deadline-for-application-of-strong-customer-authentication-for-card-payments-in-e-commerce-transactions-to-31-12-2020/ (accessed 30 January 2020).

Legislative Materials

ErläutRV 207 BlgNR 24. GP.

ErläutRV 11 BlgNR 26. GP.

IA 2284/A 25. GP

Thierry Bonneau[1]
(University Paris)

THE TRANSPOSITION OF THE PSD2 IN FRANCE

1. One of the main features that characterises the way European texts are implemented in France lies in the attempt to avoid a formal vote of the French Parliament on the text. It is not, however, possible to stave it off totally. A law is needed to authorise the government to adopt the text instead of the Parliament, that is to say enabling legislation that empowers the government to adopt the ordinance that will transpose the European text.

2. This process has one objective: to prevent the French parliament from modifying the content of the European text. This point only concerns the Parliament. It doesn't mean that the European text will be implemented in a compliant way by the government. Experience shows the opposite. One should know that the provisions about what is commonly called "cash-back", set out in article 3 (e) of the directive of 25 November 2015[2], were not transposed in the ordinance of 9

[1] Agrégé des facultés de droit - Professor of Law at the University Paris 2 (Panthéon-Assas).

[2] 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. See in particular, Th. Bonneau, La directive sur les services de paiement 2 : révolution ou évolution ?, Journal de droit européen juin 2016 n° 230 p 214 ; Régulation bancaire et financière européenne et internationale, Bruylant, 5° éd. 2020, n° 467 et s.

August 2017[3], which is the main text for the transposition of the PSD2. These provisions were implemented laterly, by the law of 3 August 2018[4].

3. This law is not only vital for this reason. There is another reason, connected to the main means used for the transposition. It is clear that an enabling law is needed initially as I have underlined: as far as the directive of 25 November 2015 is concerned, the enabling law was a law of 9 December 2016[5]. However, after the adoption of the ordinance, a ratification law in order to consolidate the ordinance is required. The law of 3 August 2018 is the text which consolidates the ordinance of 9 August 2017.

---

[3] Ordonnance n° 2017-1252 du 9 août 2017 portant transposition de la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché. V. J. Lasserre Capdeville, Nouvelle réforme des services de paiement : la « DSP2 » est transposée, JCP éd. G, 922 ; P. Storrer, Notice explicative de l'ordonnance de transposition de la DSPS (et appendice), Rev. Banque 2017, n° 812, p 79 ; P. Storrer et M. Roussille, Transposition de la DSP2 en droit français : morceaux choisis, Banque et droit 2017, n° 175, p 52 ; K. Magnier-Merran, La « DSP2 » et les nouveaux services de paiement : chronique d'une « démonopolisation » bancaire annoncée, Rev. dr. bancaire et financier mars-avril 2018, Dossier 7 ; Th. De Ravel d'esclapon, Le renforcement de la protection des informations intéressant l'uilisateur de services de paiement, Rev. dr. bancaire et financier mars-avril 2018, Dossier 8 ; C. Kleiner, L'extension du champ d'application territoriale et monétaire des nouvelles règles sur le marché intérieur des services de paiement, Rev. dr. bancaire et financier mars-avril 2018, Dossier 9 ; J. Lasserre Capdeville, Evolution du droit intéressant les PSP : extension des exceptions à leur monopole et assouplissement de leurs règles de création, Rev. dr. bancaire et financier mars-avril 2018, Dossier 10 ; N. Kilgus, L'évolution des procédures de contestation des paiements, Rev. dr. bancaire et financier mars-avril 2018, Dossier 11.

[4] LOI n° 2018-700 du 3 août 2018 ratifiant l'ordonnance n° 2017-1252 du 9 août 2017 portant transposition de la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur. V. J. Lasserre Capdeville, De la ratification à la reconnaissance du cash-back, JCP 2018 éd. G, 920.

[5] Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite loi « Sapin 2 ».

4. The law of 9 December 2016, the ordinance of 9 August 2017 and the law of 3 August 2018 are not the only texts to consider. The law of 7 October 2016[6] has to be taken into account because it is the text which started the transposition of the directive. One should also consider the texts that explain the legislative texts: two decrees[7] and five ministerial orders[8] published in 2017.

5. Finally, the transposition of the PSD2 was implemented in three steps that corresponds to three dates: 2016 (I), 2017 (II) and 2018 (III). That explains my approach in three parts. However, one mustn't forget that the vital step is 2017 because the main text is the ordinance of 9 August 2017 whose provisions came into force 13 January 2018[9], date imposed as the deadline for the transposition by the Directive of 25 November 2015[10]. And I am conscious that, but

---

[6] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

[7] Décret n° 2017-1313 du 31 août 2017 portant transposition de la directive n° 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché ; Décret n° 2017-1314 du 31 août 2017 portant transposition de la directive n° 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché.

[8] Arrêté du 31 août 2017 modifiant l'arrêté du 29 juillet 2009 relatif aux relations entre les prestataires de services de paiement et leurs clients en matière d'obligations d'information des utilisateurs de services de paiement et précisant les principales stipulations devant figurer dans les conventions de compte de dépôt et les contrats-cadres de services de paiement ; Arrêté du 31 août 2017 modifiant l'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution ; Arrêté du 31 août 2017 modifiant l'arrêté du 20 mai 2015 portant réglementation prudentielle et comptable en matière bancaire et financière en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna ; Arrêté du 31 août 2017 modifiant l'arrêté du 2 mai 2013 portant sur la réglementation prudentielle des établissements de monnaie électronique **;** Arrêté du 31 août 2017 modifiant l'arrêté du 29 octobre 2009 portant sur la réglementation prudentielle des établissements de paiement.

[9] Art. 35, Ordinance of 9 August 2017.

[10] Art. 115, Directive of 25 November 2015.

for some provisions, the directive is a full harmonisation measure. Therefore, my closing remarks will be about the compliance of the French legislation with the EU legislation.

I – 2016

6. In 2016, there are two dates: 7 October and 9 December. I don't want to insist on the article 70 of the law of 9 December 2016 because of its limited range: the authorisation given to the government to take the measures required for the implementation of the directive. By contrast, I want to say a word about the law of 7 October 2016.

7. The main objective of this text is not the transposition of the directive. This text has another objective: to take into account the development of the internet. Such a theme is relevant when it comes to payment services because of the increasing importance of electronic payments. The PSD 2 has considered the new types of payment services online, particularly the services offered by electronic communications operators (SFR, Orange, Bouygues Telecom, etc) such as online purchases (electronic theatre tickets for instance) mentioned on the bills of their clients. The idea is to make these payments easier, which implies excluding, from the scope of payment services, the services offered by electronic communications operators: it is the aim of article 3, l, of the Directive 25 November 2015. This exclusion is introduced in the French legislation by the law of 7 October 2016 : its article 94 is the basis of the new article L. 521-3-1 of the monetary and financial code, which sets out the conditions applicable to the exclusion.

II – 2017

8. In 2017, there were eight texts: one ordinance, two decrees and five ministerial orders. These texts modified the legislative and regulatory sections of the French monetary and financial Code as

well as some existing ministerial orders, notably orders concerning the prudential regulation[11]. Some of these texts were amended by some more recent texts[12], which haven't affected the provisions implementing the directive of 25 November 2015.

9. Decrees and ministerial orders are not without interest. In particular, the objective of one of them is to impose on account information service providers the internal control obligations. This observation leads me to underline the fact that some texts are specific to payment service providers – it is the case for the ministerial order devoted to the prudential regulation applicable to these professionals – while others are not specific to them. They may concern other professionals such as credit institutions. It is the case of the ministerial order of 3 November 2004 concerning the internal control. It is also true about the monetary and financial Code which is about the banking and financial sector. However, this observation must be put in perspective because there is a section devoted to payment service providers in the legislative and regulatory sections of the code. The ordinance of 9 August 2017 modified the legislative section; the two decrees of 31 August 2017 amended the regulatory section.

10. I don't want to insist on the decrees because, from a quantitative point of view, they are not so important and because they only give details for the application of the legislative section.

---

[11] See the texts mentioned in footnote 6.

[12] See : Arrêté du 31 août 2017 modifiant l'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution ; Arrêté du 31 août 2017 modifiant l'arrêté du 29 juillet 2009 relatif aux relations entre les prestataires de services de paiement et leurs clients en matière d'obligations d'information des utilisateurs de services de paiement et précisant les principales stipulations devant figurer dans les conventions de compte de dépôt et les contrats-cadres de services de paiement ; Arrêté du 31 août 2017 modifiant l'arrêté du 29 octobre 2009 portant sur la réglementation prudentielle des établissements de paiement.

The only thing that I would like to underline is that you will find, in this section, the definitions of payment services[13]. This point has to be mentioned because other definitions, such as the definition for the authentication of clients[14], are set out in the legislative section. It is difficult to explain this approach that leads to the dissemination of provisions that seem equivalent to each other.

11. The legislative section was mainly amended by the ordinance, which is the main text for the transposition of the directive of 25 November 2015. However, one should be aware of the fact that some provisions of the ordinance don't concern the transposition of the directive. They only ensure the application of the monetary and financial Code to some specific French territories such as New Caledonia and the community of Saint-Barthélemy.

12. 21 articles of the ordinance are devoted to the transposition. This number may surprise because of the number of articles of the directive of 25 November 2015. However, one should go beyond this appearance. A quick look at the content of the articles clearly shows that the reform is not limited. Each article of the ordinance modifies several texts of the monetary and financial Code: for instance, article 2 of the ordinance is made up of 32 items and some of these points modify several articles of the monetary and financial Code. What's more, one knows that the directive doesn't revolutionize the legal framework. That explains that the structure of the Code, that is to say the way provisions are organised in several books, is not affected. Only a few new sections were introduced. However, It is important to mention that the European provisions are not concentrated in one book of the code. They are disseminated in several books: 1 (money), 3 (services), 5 (service providers) and 6 (institutions for the banking and financial sector).

[13] Art. D. 314-2, Monetary and financial Code.

[14] Art. L 133-4, Code above mentioned.

13. This approach, rather formal, is not sufficient in order to enlighten the way was the PSD2 implemented in France. To this approach must be added a more substantial approach. From this point of view, it seems vital to underline the mains subjects addressed by the ordinance of 9 August 2017.

14. I can give several examples: relationships between payment initiation service providers, account information service providers and account servicing payment service provider[15], rules of access to payment accounts[16], payment transaction whose amount is not known in advance[17], Authentication[18], claim processing[19], administrative sanctions[20], professionals' access to personal data[21], registration of account information service providers[22], European passport for payment service providers[23], authorisation and simplified authorisation of Electronic money institutions[24], European passport of Electronic money institutions other than French institutions[25]. These items addressed by the ordinance are only examples and are the most obvious when you read the ordinance. Other modifications are less clear; a comparative reading of the text in its version before the ordinance and of the modified text is necessary in order to be aware of the changes, resulting from the PSD2, in the French legal framework.

---

[15] Art. L 133-17-1.

[16] Art. L 133-39, L 133-40 and L 133-41.

[17] Art. 133-42 and L 133-42.

[18] Art. L 133-44.

[19] Art. L 133-45.

[20] Art. L 171-1,L 171-2 and L 171-3.

[21] Art. L 521-5, L 521-6, L 521-7 and L 521-8.

[22] Art. L 522-11-2 and L 522-11-3.

[23] Art. L 522-12.

[24] Art. L 526-9 and L 526-19.

[25] Art. L 526-24.

15. Therefore, it is not easy to assess the compliance of the French law with the Directive of 2015. It is true that the main changes were introduced in the French legislation[26]. The new payment services – the payment initiation service and the account information service – are in our legislation. The same observation is true as far as the claim processing and the security of payment, through the authentication, are concerned. However, not all the provisions of the EU legislation are in the French Code. For instance, some definitions haven't been introduced. It is the case for the definition given for the payment order by article 4, 13, Directive of 2015: this definition is not in the French legislation while the definitions given for payment account[27] and payment transactions[28] are mentioned. That is surprising because a definition is a basic element that determines the extent of the legislation. It is all the more open to criticism because there is no option for member states not to take into account article 4 of the PSD2.

16. The same observation is true as far as article 3 of the directive is concerned. Some of its provisions were not considered. The law of 3 August 2018 contributed to improving the transposition of the PSD 2 in the French legislation.

III – 2018

17. In 2018, there is only one text already mentioned: the law of 3 August. This text was adopted after the deadline imposed by the directive: 13 January 2018. However, its scope is really limited as regards the implementation of the PSD2. The transposition is only about the practice called "cash back".

---

[26] See Lasserre Capdeville, Nouvelle réforme des services de paiement : la « DSP2 » est transposée, paper already mentioned.

[27] Art. 4, 12), Directive and art.L 133-3, I, Monetary and financial Code.

[28] Art. 4, 5), Directive and art.L 314-1, I, Monetary and financial Code.

18. This practice is covered by article 3 of the PSD 2 entitled "exclusion". The objective of the directive is to authorise the possibility for a client to pay by card an amount above the price really owed in order to get cash from shopkeepers. This exclusion was not taken account by the ordinance of 9 August 2017. The law of 3 August 2018 modified the monetary and financial Code[29] in order to introduce this exclusion in the French legislation.

19. This law[30] modified other texts, such as article L 133-28 that is about instruments reserved to payments of low amount. This text must be combined with article D 133-7. It results from both these texts that France has not used the option to reduce or double the amounts mentioned in article 42 of the PSD2.

20. A similar observation can be made about article L 314-13, modified in 2017, part IV of which concerns the termination of the framework contract. France has not used the option set out in article 55, § 6 according to which "Member state may provide for more favourable provisions for payment service users".

21. The last examples show again how difficult it is to assess the compliance of the French legislation with the EU legislation. At the very least, on one point, the compliance is still not total[31]. However, and despite the difficulty resulting from the fragmentation and the dissemination of the European provisions in the French legislation as well as the difficulty of monitoring the exercise of the options offered to member states by article 107 of the PSD2, it seems that the transposition is globally correct and that the objective of harmonisation has been reached.

---

[29] Art. L 112-14, Code above mentioned.

[30] Art. 4, Law of 3 August 2018.

[31] See, about définitions, supra § 15.

Vittorio Santoro
(Università di Siena)

CONSIDERAZIONI CONCLUSIVE

1. La PSD 2 si sviluppa secondo le seguenti tre direttrici, collegate fra loro:

1) aumentare la difesa dei consumatori;
2) consentire lo sviluppo della tecnologia applicata al sistema dei pagamenti;
3) aprire il mercato dei servizi di pagamento a nuovi operatori per c.d. "tecnologicamente dotati".

Secondo gli intendimenti del legislatore le tre direttrici dovrebbero, poi, convergere verso l'obiettivo della diminuzione dei costi con beneficio finale per gli stessi utenti dei servizi.

Tutte le direttrici, così come le loro implicazioni e connessioni sistematiche, sono state oggetto di approfondimento nei contributi raccolti in questo volume. In particolare il prof. Freitag ci fa notare che la PSD 2 è al centro di un sistema complesso di norme e al riguardo costruisce uno schema particolarmente efficace.

Tuttavia, anche egli si concentra solo su alcuni collegamenti non mancando, però, di aprire una interessante finestra sull'*E-money* che, a suo parere, dovrebbe essere oggetto della PSD 3. L'*E-money* non dovrebbe comprendere la *cyber-currency* poiché altrimenti sarebbe compromessa la sovranità monetaria. Il punto a mio avviso deve essere condiviso e comporta la conseguenza (per molti ordinamenti, sicuramente per quello italiano) che qualora l'obbligazione sia quella di pagare in *cyber-currency* il creditore non

può chiedere l'equivalente in moneta legale, poiché non si tratta di moneta e neanche vi può essere un corso del cambio al giorno della scadenza (art. 1278 c.c.).

Nonostante la molteplicità di collegamenti evidenziati da Freitag, egli non si occupa delle connessioni della PSD 2 con la legislazione anti-riciclaggio e con quella fiscale. In Italia quest'ultimo tema è al centro del dibattito politico poiché, per motivi connessi al contrasto dell'evasione fiscale, sono state proposte soluzioni quali: a) non solo mantenere l'obbligatorietà del POS per i commercianti, ma sanzionarne la mancanza; b) concedere incentivi fiscali ai cittadini che usano carte, bancomat o, comunque, mezzi di pagamento tracciabili.

Personalmente credo che, per essere effettivamente favorito, l'uso di mezzi di pagamento alternativi al contante dovrebbe essere fiscalmente neutro, così si dovrebbe sopprimere il balzello sugli estratti di saldaconto e la piccola patrimoniale sulle consistenze depositate in banca.

2. I temi, poco prima enumerati, sono stati in varia misura ripresi nei contributi dei colleghi stranieri.

Apprendiamo molto da Guimarães, Steennot, Bonneau (ma un po' da tutti gli autori di altri paesi) sia in termini di omogeneità di regole attuative che di loro interpretazione. Emergono, tuttavia, anche alcune differenze che mi inducono a ricordare e condividere una notazione di Linardatos secondo il quale le incertezze (e dunque anche le disomogeneità tra ordinamenti europei) sono in contrasto con la costruzione di un mercato unico dei servizi di pagamento: le incertezze devono essere superate non solo nel diritto interno di ciascuno stato ma anche perseguendo un obiettivo di omogeneizzazione interpretativa tra gli stati. A tale ultimo fine, progetti di ricerca tra studiosi di diversi paesi europei, come quello che ha portato alla presente pubblicazione, possono svolgere una funzione molto utile, direi persino essenziale.

Scendo, per esemplificare, in due casi di dettaglio: 1) Steennot racconta che, in Belgio l'Ombudsfin non riconosce il diritto al risarcimento alle persone quali sia rubata la carta di pagamento mentre usufruiscono di una camera d'albergo, di un letto d'ospedale o

viaggiano su un treno poiché l'Ombudsfin ravvisa sempre una grave negligenza nel comportamento, supponiamo, di una vecchia signora che non adotti la medesima cura nella custodia della carta, adottata, invece, nella custodia dei gioielli depositati in cassetta di sicurezza prima del ricovero ospedaliero. Non è sempre così nelle decisioni italiane, è nota l'opinione opposta dell'Arbitro bancario e finanziario che ritiene inevitabile che i degenti in ospedale portino con sé le carte per eseguire le piccole spese quotidiane, non avrebbe senso pretendere che si riponga la carta di pagamento nella cassetta di sicurezza così come si farebbe per i gioielli; 2) Linardatos, a sua volta, sostiene che in caso di furto o smarrimento della carta, in Germania si presume che i codici siano custoditi insieme con la carta ben oltre il tempo ristretto (circa quindici minuti) in cui la stessa presunzione vale nelle decisioni dell'ABF italiano. E, in verità, questa volta l'interpretazione tedesca mi sembra più ragionevole.

Ritornando a un piano più generale, credo sia importante rammentare la notazione di Miernicki che sostiene che le disposizioni che, nell'ordinamento austriaco, le disposizioni regolanti i servizi di pagamento non costituiscono legge speciale bensì generale; mi sembra che la stessa cosa valga anche per l'ordinamento tedesco ove il legislatore ha inserito alcune disposizioni nel BGB e, in particolare, nell'ambito del *Geschäftsbersogungsvertrag*, *ex novo* la disciplina dell' *Überweisungsvertrag* (§ 676a e ss.) e dello *Zahlungsvertrag* (§ 676d e ss.)

Io credo che, anche negli altri ordinamenti, il legislatore dovrebbe prestare attenzione al fine di riportare le disposizioni in tema di servizi di pagamento ai principi civilistici generali, se del caso, inserendo o riformando alcune norme delle codificazioni nazionali (e si confronti anche il punto di vista di Minneci).

A me sembra che il tema sia particolarmente urgente e importante per quanto riguarda l'allocazione della responsabilità contrattuale nei rapporti tra utente e fornitore di servizi di pagamento (sul punto si vedano i contributi di Olivieri e Minneci). Il tema della responsabilità non può prescindere da una collocazione sistematica delle relative disposizioni (si veda anche il contributo di Mezzacapo).

Si deve poi riflettere se taluni per c.d. "automatismi", previsti nella relazione utente fornitore di servizi di pagamento non debbano essere riferiti e risolti per mezzo di una diversa, e non abituale, qualificazione della fattispecie. Intendo dire qualificando il contratto quale di servizio e, pertanto, avente ad oggetto la prestazione di un risultato e non una prestazione di mezzi. Ciò, va da sé, salvo che al prestatore del servizio di pagamento non sia stata richiesta un'attività aggiuntiva e particolare come si è esemplificato nella giornata di ieri con riguardo ai pagamenti internazionali delle società petrolifere.

3. Le questioni relative all'innovazione tecnologica sono state affrontate, in modo particolare, dagli autori della prima sezione tra entusiasmi (moderati) e riferimenti alle preoccupazioni di alcuni operatori che potrebbero mettere in campo alcune strategie "difensive".

La banca tradizionale e/o di modeste dimensioni che, rispettivamente, non voglia, oppure non sia in grado di affrontare i notevoli costi che richiedono l'innovazione tecnologica, potrebbe scegliere di fornire esclusivamente un'operatività non *on-line,* coltivando una clientela tecnologicamente analfabeta (ad es. perché anziana) o diffidente delle novità tecniche in quanto ritenga (a torto o a ragione) che la esponga ad indebite intrusioni nella sfera privata.

Gli operatori di settore potrebbero disegnarci uno scenario nel quale nel giro di tre anni questa realtà tradizionale sarà spazzata via, non dubito che questo sia il futuro che ci attende, dubito che i tempi saranno così rapidi se non altro perché vedo che le persone anziane (che sono anche quelle con patrimoni cospicui) traggono troppo piacere da quattro chiacchiere con il cassiere o il funzionario di turno.

È più probabile che, nel medio termine, la banca tradizionale cooperi con società tecnologicamente avanzate per offrire al cliente l'opportunità di servizi più avanzati. In tal senso depongono importanti segnali rilevati dall'Osservatorio Fintech & Insurtech del Politecnico di Milano secondo il quale "Le evidenze mostrano come una collaborazione con le *fintech* rappresenti un'opportunità per gli

incumbent [leggi le banche] di sviluppare nuovi modelli di business e rimanere competitivi facendo leva sui nuovi paradigmi dettati dall'innovazione tecnologica, elemento fondamentale per soddisfare le esigenze e le necessità dei consumatori".

La Banca d'Italia si sta preoccupando e preparando per governare entrambi gli scenari: quello della banca che rimane tradizionale e quella che affronterà più rapidamente l'innovazione tecnologica.

4. Qui si apre il vero tema nuovo, implicito nelle disposizioni della PSD2, vale a dire quello della concorrenza "distruttiva" del sistema bancario tradizionale.

I nuovi operatori, come scrive Pozzolo, sono i vincenti di domani, con un uso appropriato delle nuove tecnologie offriranno la possibilità di portare a termine un pagamento facile, veloce e sicuro, persino in un unico *step*: la prospettiva è di superare l'attuale segmentazione delle operazioni di pagamento, anche andando oltre l'abituale schema delegatorio.

C'è, tuttavia, qualcosa che non torna (come si legge nell'introduzione dei curatori); infatti, anziché livellare il terreno di gioco tra operatori vecchi (banche) e nuovi (società *fintech*), corriamo il rischio di mettere fuori mercato le banche poiché solo esse sono onerate dei più gravosi costi di vigilanza. A questo punto sarebbe meglio, al fine dell'equilibrio concorrenziale, seguire l'evocato consiglio di Bill Gates ed elaborare un nuovo concetto di banca che comprenda operatori tradizionali e innovativi da sottoporre alla medesima disciplina.

Per valutare la rilevanza sistematica delle scelte di politica legislativa è bene ricordare che, al fine del livellamento del piano di gioco, sulle due sponde dell'Atlantico si seguono due itinerari opposti: negli US si è a lungo ritenuto opportuno ridurre le regole per tutti gli operatori, dopo la parentesi conseguente alla crisi economica, questa strada sembra in ripresa; in Europa la concorrenza fra banche si è sempre svolta nel quadro di un mercato fortemente regolato, ma nuovi operatori (e qui sta l'asimmetria segnalata

nell'introduzione) possono svolgere una parte sempre più ampia della tradizionale attività bancaria subendo solo una supervisione per c.d. *light*. Un solo esempio, a fronte di regole di patrimonializzazione sempre più gravose per le banche, gli ultimi entranti i «prestatori di servizi di disposizione di ordine di pagamento" possono limitarsi a stipulare una polizza per assicurare l'eventuale responsabilità per danni a terzi.

Ma chi si appresta a entrare in questo "nuovo" mercato dei servizi di pagamento? Non certo solo modesti e intraprendenti operatori, ma piuttosto colossi della tecnologia e delle comunicazioni solitamente basati proprio negli US (della cui visione più liberare per giunta si giovano), i primi nomi sono: Google, Netflix, Uber, Airbnb, Spotify, Twitter, Facebook, Instagram, Amazon, eBay, PayPal ecc. a cui si deve aggiungere la presenza di colossi cinese quali Alibaba e Baidu, non certo più tranquillizzanti sotto il profilo concorrenziale per le banche europee.

Questi operatori possono entrare nei dati delle banche senza ostacoli sostanziali. In verità al di là dell'accesso legale nei limiti in cui oggi gli è consentito, i colossi dell'informatica hanno la tecnologia per praticare, fra l'altro, il c.d. *scraping* che è una tecnica di raccolta dati che consente a un sistema informatico di "raschiare" i dati visualizzati sullo schermo o su un altro dispositivo di *output* di un secondo sistema informatico. I dati legittimamente o illegittimamente acquisiti possono essere poi combinati con una serie infinita di altri dati già in loro possesso.

Di fronte alla forza tecnica ed economica delle imprese, che ho prima ricordato, sono comprensibili le preoccupazioni espresse da più parti in dottrina e, allo stesso tempo, risultano quasi ridicole alcune disposizioni quali quelle che prevedono che i nuovi operatori non devono chiedere "al pagatore dati diversi da quelli necessari per prestare il servizio di disposizione di ordine di pagamento" né usare, conservare e accedere ai dati «*per fini diversi dalla prestazione del servizio di disposizione di ordine di pagamento e non conserva dati sensibili relativi ai pagamenti del pagatore*».

5. Guardando alla disposizione appena ricordata, da un diverso punto di vista cioè quello della legislazione antiriciclaggio e antiterrorismo, essa potrebbe essere considerata persino controproducente.

Infatti, le grandi multinazionali *fintech*: 1) da un lato, non sono destinatarie di obblighi di collaborazione con le Autorità di informazione finanziaria ai fini della prevenzione del riciclaggio e del terrorismo, laddove persino i tabaccai hanno alcuni oneri al riguardo; 2) dall'altro qualora, quali "nuovi" operatori nei servizi di pagamento, entrino in possesso "di informazioni sensibili", invece di segnalarle alle Autorità, dovrebbero disfarsene!

La soluzione mi lascia perplesso perché le grandi multinazionali *fintech* gestiscono i *big data* e, pertanto, dispongono di informazioni ben più complete di quanto possa averne qualsiasi banca, esse sono in grado di sorvegliare i flussi di danaro, basta vedere qualsiasi telefilm poliziesco americano per rendersi conto di quale fonte di informazione essi siano. Solo partendo dal dato della realtà possiamo, poi, preoccuparci che la gestione delle informazioni sia rispettosa della *privacy* dei cittadini.

6. Ancora sotto il profilo del diritto della concorrenza, Olivieri, nel suo contributo, ci ricorda l'obiettivo del legislatore europeo a favore dell'ampliamento della gamma dei prodotti e dei soggetti operanti nel campo della prestazione dei servizi di pagamento soffermandosi sul contenuto degli artt. 66 e 67 della PSD 2 (rispettivamente recanti «*Disposizioni per l'accesso ai conti di pagamento in caso di servizi di disposizione di ordine di pagamento*» e «*Disposizioni per l'accesso alle informazioni sui conti di pagamento e all'utilizzo delle stesse in caso di servizi di informazione sui conti*».

Condivido le sue considerazioni, ma qui voglio riferirvi di una posizione eccentrica che ho letto in uno studio di Ghidini e Di Porto i quali hanno affermato: «*proactive antitrust enforcers could identify each and every customer's account data as a separate relevant market*», affermazione più avanti temperata dalla reciproca nei confronti dei conglomerati *fintech*, i quali dovrebbero a loro volta concedere l'accesso ai propri dati alle banche.

Che anche l'accesso ai conti di un singolo cliente della banca sia da considerare obbligatorio perché si tratterebbe di un'*essential facility* è per me duro da accettare. Credo che le disposizioni, che stiamo esaminando, non siano frutto delle categorie del diritto europeo *antitrust*, benché sia allo stesso tempo indubbio che il legislatore europeo vuole forzare le banche in modo da rompere una posizione preminente sul mercato, ma a prescindere da dall'abuso di una posizione dominante sul mercato. Circostanza, quest'ultima, che è resa evidente dal fatto che gli articoli 66 e 67 si applicano a tutte le banche, anche a una modesta banca locale, quindi indipendentemente dalla posizionamento rilevante che la banca abbia sul mercato.

Vittorio Santoro
(Full professor of Commercial Law University of Siena)

CONCLUDING REMARKS

1. The PSD 2 pursues three strictly correlated objectives:

1) enhancing the consumers' protection;
2) enabling the development of technology in the context of payment systems;
3) granting the access to the market of payment services to new businesses which are "technologically equipped".

According to the intentions of the EU legislator, the above objectives should strengthen the more general goal of reducing costs for the benefit of the same users of the various services.

All these functions, together with their relevant implicantions as well as systematic ramifications, have been expanded upon and investigated by the Authors of this volume. In particular, prof. Freitag draws our attention to the fact that PSD 2 is, at its core, a complex system of norms and, to this respect, it provides a very effective framework.

However, prof. Freitag, together with other authors, focuses on some of these implications, without omitting the interesting perspective concerning E-money. E-money, he suggests, should be further regulated by the next PSD 3. In this sense, prof. Freitag believes that the regulation of E-money should not include cyber-currency as to do so would mean impairing monetary sovereignty.

I think that this position deserves to be shared and accepted. Furthermore, it implies (for many jurisdictions including Italy)

that every time the object of the contractual performance is that of paying with cyber-currency, the relevant creditor of such performance is not allowed to expect the equivalent amount payed with legal tender simply because cyber-currency is not money nor does it have an exchange rate at the date in which the relevant monetary obligation falls due (Article 1278 Italian Civil Code).

Despite highlighting the various aspects, prof. Freitag doesn't expand upon the connections between PSD 2 with anti-money laundering and fiscal legislation.

This is actually highly debated in Italy at a political level for reasons related to the contrast of tax evasion. In this vein, many solutions have been proposed such as: a) making the use of POS compulsory and sanctioning the breach of this rule for payments transacted between retail businesses and clients; b) tax incentives to consumers that, relying on cashless transactions, use credit cards, debit cards or payment instruments that are traceable.

Personally I think that methods of payment alternative to cash should be encouraged by considering them neutral from a fiscal point of view so that both any stealth tax applied to accounts and the minor but nevertheless still a tax on assets applied to deposits held should be cancelled.

2. The above-mentioned aspects have been discussed in various instances by other foreign contributors.

We learn a lot from proff. Guimarães, Steennot, Bonneau (actually, from almost all the foreign contributors, without exceptions) about the difficulty of ensuring the uniformity of the legislation in question when considering its interpretation and application. Some discrepancies, however, are coming to the surface and this reminds me of a rather prophetic remark from prof. Linardatos according to whom uncertainties (and therefore the consequent disharmonization amongst European member jurisdictions) fly in the face of the very idea of creating a single market of payment services. In this sense, Prof. Linardatos emphasizes that uncertainties must be dealt with and

overcome not only at the single-EU Member State level but also by pursuing an effectively consistent and uniform interpretation of the same legal framework amongst EU Member States. In fact, research projects which involve various academics from different Member States – projects similar to that which have led to this publication – may well bring a useful, even essential function to fruition.

Amongst the many, I feel that two cases in particular demonstrate this. Steennot reports that the Belgian "Ombudsfin" does not allow damages to those users whose payment instrument has been stolen whilst, for example, sojourning in a hotel, being hospitalized or travelling on a train. In this case, the "Ombudsfin" deems this conduct to be negligent rather like that of an elderly woman adjudged to have not employed the same level of care and diligence (when dealing with a payment instrument such as the card) as she would use with her jewellery being deposited in a safety deposit box before being hospitalized. It is true that the Italian "Arbitro Bancario e Finanziario" (ABF) does not take the same view as it states that elder patients should be inevitably allowed to take payment instruments to make daily small-value transactions. Indeed, the Italian ABF deems that it would not be reasonable to expect that the same patients keep their payment instruments in a safety deposit box as they would do with their jewellery. At the same time, prof. Linardatos suggests that in Germany, in the event of theft or loss of the payment instrument, the judicial authority moves from the premise that this payment instrument had been kept together with the relevant codes when, between the unauthorized access to the account (by a thief) and the withdrawal of money via the use of the same payment instrument, there is a lapse of time which exceeds 15 minutes, On the contrary, the Italian ABF does not allow the same presumption in the event the same lapse of time exceeds this time limit. In truth, it seems to me that the German interpretation is more reasonable.

At a more general level, I think that it is worth mentioning the remark of prof. Miernicki concerning the fact that within the Austrian jurisdiction the norms that regulate payment services do not

rank nor operate as special provisions but rather they concur to form the general legal framework. My understanding is that the same approach is adopted by the German jurisdiction where the legislator has modified the BGB by enacting some provisions in relation to the *Geschäftsbesorgungsvertrag* and by regulating either the *Überweisungsvertrag* (§ 676a ff.) or the *Zahlungsvertrag* (§ 676d ff.)

I also believe that in other jurisdictions the legislator should carefully consider bringing the legal framework on payment services within the general legal framework of civil law by modifying, if necessary, the relevant Civil Codes (please, see prof. Minneci's contribution for an appropriate in-depth analysis).

Furthermore, I think that this perspective is of paramount importance and urgency when it comes to dealing with the issue of allocating transactional costs, mainly the costs of liability, between the payment service user and the payment service provider (please, see the contributions by professors Olivieri and Minneci). In fact, an efficient and systematic approach to the issue of liability cannot leave aside the fact that the relevant norms must be given an equivalent, corresponding general purview (please, see the contribution by prof. Mezzacapo).

I also feel that there is the need to emphasize the fact that certain automatic aspects and effects that the law sets out with respect to the relationship between the payment service user and the payment service provider should be assessed in accordance with a case-by-case analysis of the relevant facts. Then, any contract of payment services should be classified in light of the fact that it governs a performance for a service. It follows that it should be intended as vesting the creditor of such performance with the right of expecting a specific result, *i.e.* a particular service, rather than with the sole right of expecting that the same service will be carried out with reasonable care and skill. This, unless the payment service provider is required to perform an additional obligation, as was discussed on the first day of this symposium with respect to international payments due by oil companies.

3. The issues relating to innovation technology were dealt with by the authors of the first session which made reference to conceivable enthusiasm (though moderate) but also warned about the fact that certain service providers might employ various "defensive" strategies.

A small-sized bank which does not intend to, or is not able to, afford the considerable costs relating to innovation technology might decide to carry out its business almost exclusively off-line. In this sense, this bank might then decide to invest in clients who are technologically illiterate (for instance, elderly people) or sceptical about new technologies mainly because these clients believe that thinking otherwise would result in their disproportionate, undue exposure to unwanted interferences regarding their privacy.

Banking experts may well draw a scenario within which this traditional approach will be completely eradicated. I have no doubt that this is going to be the future context; in the other hand, I seriously doubt that this is going to happen any time soon, if nothing else because elderly people (more often than not, high-net-worth individuals) take pleasure in speaking to and dealing directly with a bank clerk at their local premise (rather than interfacing with a computer) for clarification or information.

It is more likely that in the short to medium term these traditional banks are willing to cooperate with technologically advanced businesses in order to offer their clients more sophisticated services they are not equipped to offer directly. This is confirmed by "Fintech & Insurtech" of the Politecnico of Milan according to which "Evidence shows that the cooperation with *fintech*-buisinesses is an opportunity for the incumbents [banks] to develop new competitive business models and to remain competitive by taking advantage of the new paradigms of innovation technology, which is a fundamental element to meet the needs and the necessities of consumers".

The Bank of Italy is working hard to manage both scenarios: the bank which continues to operate as a traditional bank, on one side, and that of the bank which will embrace and deal with innovation technology, on the other.

4. It is here that a new issue arises, that is the issue implied by PSD 2: I specifically refer to the disruptive competition affecting the traditional banking system.

Those operating within the most advanced banking systems, in the words of prof. Pozzolo, will be tomorrow's winners. They, with the appropriate use of new technologies, offer the possibility to complete a payment safely, quickly and in one easy step: the suggested approach is that of overcoming the current fragmentation of the payment transactions by also rejecting the idea of a transaction structured on the basis of a mandate.

However, there is something fundamentally wrong (as we read in the introduction by the editors); indeed, instead of creating a level playing field for traditional businesses (banks) and new businesses (fintech businesses), we run the risk of expelling banks from the market as they are the only ones expected to bear the brunt of the heavy costs of supervision.

At this point it would be better, in order to favor a balanced competition, to follow the suggestion of Bill Gates and to think of a new concept of banking that includes both traditional and new players under the same legal umbrella.

In order to evaluate the ramifications of the legislative policy it is worth remembering that, with the objective of creating a level playing field, the two extremities of the U.S., East and West, follow two opposite itineraries: the U.S. system has always favored an element of deregulation for the benefit of all the players. And, following the crisis this concept appears to be more appealing. Conversely, in Europe the competition between banks has always been heavily regulated and controlled. In this context, however, new players (and here is the asymmetry highlighted in the introduction) can carry out an increasing part of the traditional banking activity under "light supervision".

One example captures this asymmetry.

Whereas the banks are subject to an increasing number of restrictions concerning their level of capitalization, the new payment ini-

tiation service providers are only required to take out an insurance policy to cover their potential liability towards third parties.

But who is interested in this new market of payment services? Certainly not those only interested in carrying out this business who do not possess the appropriate preexisting business structure. Rather, those who have the potential to enter this market successfully are the technology and communication giants typically based within the U.S., such as: Google, Netflix, Uber, Airbnb, Spotify, Twitter, Facebook, Instagram, Amazon, eBay, PayPal etc. In addition to these players, we should also not forget the Chinese corporations of Alibaba and Baidu, who certainly are no less aggressive than the former with respect to European banks.

These fintech businesses can enter the databases of banks without any substantial obstacles or difficulty. In reality, in addition to what the law already permits them to do, these tech giants have the know-how "to scrape", that is the technique of absorbing and collecting data as soon as it appears on the screen of a different source. It goes without saying that this data may be legally or illegally combined together with other data which is already in the hands of the same scraper-tech giants.

Conceivably, the economic and organizational power of these giants raises legitimate concerns, which indeed have been widely shared by academics. At the same time, no credibility should be given to some provisions, design to curb this intrusiveness, such as that according to which «*The payment initiation service provider shall not request from the payment service user any data other than those necessary to provide the payment initiation service*» (art. 66, paragraph 3 (f) PSD 2), and «*not use, access or store any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer*» (art. 66, paragraph 3(g) PSD 2).

5. In fact, when viewed from the perspective of anti-money laundering and antiterrorism legislation, these two provisions may appear to be somewhat counterproductive.

Indeed, multinational corporations dealing with fintech: 1) on the one hand, are not accountable nor subject to Financial Information Authorities to avert money laundering and terrorism, something that appears to be unacceptable in light of the fact that even tobacconists have certain duties regarding the same matters; 2) on the other hand, in their capacity as new players dealing with payment services, they can collect sensitive information which the law requires them to destroy once and for all instead of communicating with the Authorities!

This is buffling to say the least.

These tech giants dealing with *fintech* manage *big data* which means that they may well rely on certain informations which are much more exhaustive than those owned by the banks: they can easily monitor cash-flows (as we can learn simply by watching one of the many American movies). The inevitable approach to embrace is therefore that which evaluates reality as the starting point because only in this way is it appropriate to deal with the problem concerning how to manage information without interfering with people's *privacy*.

6. Prof. Olivieri, in his contribution that takes the antitrust perspective, emphasizes the objective of the European legislator (as it is in his opinion suggested by articles 66, titled «*Rules on access to payment account in the case of payment initiation services*», and 67, titled «*Rules on access to and use of payment account information in the case of account information services*» of the PSD 2) to promote the enlargement of the array of products and players dealing with payment services.

I certainly share his view.

At the same time, I feel the need to bring up the rather eccentric opinion expressed by professors Ghidini and Di Porto according to which: «*proactive antitrust enforcers could identify each and every customer's account data as a separate relevant market*», a statement which is soon extended to fintech corporations in the sense that they should also grant banks access to their data.

I struggle to accept the idea that access to *each* (!) bank account should be intended as an *essential facility*. I think that both articles 66 and 67 of the PSD 2, that we are examining, are not the products of antitrust law, even though it is quite clear that the legislator wants to eliminate the pre-eminent position of banks within the market. In any event, the European legislator pursues this objective regardless of the aspect concerning the abuse of the dominant position. And this is made clear by the fact that both, article 66 and article 67 of the PSD 2 apply to every bank, even to a small-local bank: that is, to any bank without considering its position within the market.

CONTRIBUTORS

Prof. Elisabetta Bani
Ordinario di Diritto dell'economia nell'Università degli studi di Bergamo

Prof. Thierry Bonneau
Agrégé des facultés de droit – Professor of Law at the University Paris 2 (Panthéon-Assas)

Prof. Vincenzo De Stasio
Ordinario di Diritto commerciale nell'Università degli studi di Bergamo

Prof. Robert Freitag
Maître en droit (Bordeaux), Professor of Law at the Friedrich-Alexander-Universität Erlangen-Nürnberg, Judge at the Higher Regional Court of Nuremberg

Prof. Maria Raquel Guimarães
Professor of Civil Law and Contract Law, Faculty of Law, University of Porto, Portugal – Centre for Legal and Economic Research

Dr. Dimitrios Linardatos
Post-Doc (Habilitand) at the University of Mannheim and Lecturer at the Mannheim Business School (Commercial and Capital Markets Law)

Prof. Simone Mezzacapo
Associato di Diritto dell'economia nell'Università degli Studi di Perugia – Membro del Financial Services User Group (FSUG) della Commissione Europea

Dr. Martin Miernicki
University Assistant (post doc), Department of Business Law, University of Vienna

Prof. Ugo Minneci
Ordinario di Diritto commerciale all'Università degli studi di Milano Statale – Membro supplente del Collegio di Milano dell'Arbitro Bancario Finanziario

Prof. Gustavo Olivieri
Ordinario di Diritto commerciale nella Facoltà di Giurisprudenza dell'Università LUISS - Guido Carli di Roma

Prof. Alberto Franco Pozzolo
Ordinario di Economia Politica nell'Università degli Studi Roma Tre – Membro supplente del Collegio di Roma dell'Arbitro Bancario Finanziario

Prof. Vittorio Santoro
Ordinario di Diritto commerciale nell'Università di Siena

Prof. Antonella Sciarrone Alibrandi
Ordinario di Diritto dell'economia nell'Università Cattolica di Milano

Prof. Reinhard Steennot
Financial Law Institute, Ghent University – Consumer Law Institute, Ghent & Antwerp University – Member of the Supervisory Board of the Belgian Financial Services Market Authority

Questa pubblicazione è stata realizzata utilizzando carta fabbricata nel pieno rispetto dell'ambiente senza l'utilizzo di sostanze nocive e con l'impiego di prodotti ecocompatibili nella fase di stampa e confezione.

Finito di stampare
nel mese di febbraio 2021
sestanteinc - Bergamo

Dietro all'uso delle carte di pagamento, delle carte di credito, dei nuovi servizi di disposizione di ordine e di informazione sui conti, così immediato da parte dell'utente, si celano complessi problemi giuridici e tecnologici, la cui soluzione ha consentito di dare rapidità di esecuzione e sicurezza sempre maggiore all'operazione di pagamento.

ISBN-978-88-6642-368-3