Zeszyty Naukowe Uniwersytet Ekonomiczny w Krakowie

8 (968)

ISSN 1898-6447
Zesz. Nauk. UEK, 2017; 8 (968): 25–42
DOI: 10.15678/ZNUEK.2017.0968.0802

Jan Byrski

Consumer Protection under Directive 2015/2366 on Payment Services in the Internal Market – Selected Issues

Abstract

Directive 2007/64 on payment services (PSD 1) introduced protection for consumers of payment services. First and foremost, the consumer should receive the basic information required by law before and after the execution of a payment. Secondly, the consumer is made more familiar with the charges incurred when paying in shops, including online shops. Third, PSD 1 provided the protection of consumer rights in the event of unauthorised or incorrect charges to the consumer's payment account. Fourthly, within PSD 1 the market for payment systems was opened, thus allowing entities other than banks to provide payment services. In order to protect consumers' money, these new institutions have become subject to regulation (supervision).

The European Union legislator, when establishing a new framework for the provision of payment services in the European Union (PSD 2), reached the conclusion that existing protection for the consumer – the payment service user, was insufficient. Therefore, new legal instruments protecting the consumer have been introduced. However, upon examination a conclusion has been reached that while some of the protections should be accepted, others warrant critical review.

Keywords: PSD 1, PSD 2, payment services, consumer protection in payment services, strong authentication, strong consumer authentication (SCA).

Jan Byrski, Cracow University of Economics, Department of Civil and Economic Law, Rakowicka 27, 31-510 Kraków, e-mail: byrskij@uek.krakow.pl

1. The Adoption of Directive 2015/2366 on Payment Services (PSD 2)* and the Importance of the Changes for the Consumer in Relation to Directive 2007/64 on Payment Services (PSD 1)**

1.1. Consumer Protection in PSD 1

PSD 1 ensured uniformity of the rules on electronic payments, e.g. payments by debit cards or cash transfers in 31 European countries[1]. This means that payments can be performed throughout Europe as easily and safely as in one's own country. The directive identified in detail the information that the consumer receives and ensured that payments are made in a faster and more secure way. In addition to banks, it enabled new entities – payment institutions (or the providers of mere money remittance service – in Poland, the offices of payment service providers) to provide payment services after obtaining the appropriate permit/registration from the supervisory authority.

All types of electronic and cashless payments, from transfer orders, direct debits, card payments (including payments made using debit and credit cards), through money remittance services to mobile payments and online payments are covered by PSD 1. However, this directive does not cover payments by cash or check.

Directive 2007/64 on payment services made it easier for the user, including the consumer, to understand information regarding payment in several ways.

First, consumers must receive the basic information they need before as well as after payment is made. Before a consumer uses the service, the payment service provider should present him with its specific conditions, including the information about the provider, the elements of the payment service (such as the procedure for consenting to the transactions), the time of the implementation of the service, any spending limits, charges and information regarding rights to receive refunds. This makes it easier for the consumer to compare available options and select the offer which most suits his needs. The consumer must also be informed of any changes to the framework agreement, including any changes in fees, at least two months in advance. In addition, after each payment, the consumer receives

---

* Directive of the European Parliament and of the Council (EU) 2015/2366 of 25 November 2015 on payment services in the internal market amending Directives 2002/65/EC, 2009/110/EC, 2013/36/EU and Regulation (EU) No 1093/2010 and repealing Directive 2007/64/EC (the Official Journal of the European Union of 23 December 2015).

** 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 repealing Directive 97/5/EC (the Official Journal of the European Union of 5 December 2007).

[1] In the European Union, Norway, Liechtenstein and Iceland.

a statement listing the amount, date, and charges so that he can verify that the transaction has been completed correctly.

Second, the consumer receives more information regarding charges incurred in shops, including online shops. Payees (merchants)[2] can give discounts to consumers who pay for purchases in a manner that is more favourable to the merchant (e.g. debit cards). Merchants may also impose higher charges on the consumer for payments which force higher costs on the merchant (e.g. using business cards) – also known as surcharges – if not prohibited or restricted by national law[3].

Third, PSD 1 provided protection of consumer rights in the event of unauthorised or incorrect charges to the consumer's account. In this case, consumers are eligible for a refund in three different situations:

1) unauthorised charges – when the consumer becomes aware of unauthorised debiting, he is entitled to an immediate refund, provided that he has reported it to his payment service provider as soon as possible, and within the deadline not exceeding 13 months from the date of debiting;

2) overstatement of charges – when the consumer has authorised a payment transaction, without specifying the amount at the time of the authentication (e.g. by direct debit or payment by credit card for booking a hotel) and the actual amount of the debit charged significantly differs from what could reasonably be expected, the consumer is entitled to contest this amount by contacting the payment service provider within eight weeks. The payment service provider should then provide either the refund within ten days or the reasons for refusing to provide it;

3) incorrect processing – if the consumer has authorised a transaction, but the payment service provider makes an error processing the payment (e.g. did not process the payment, debited the account an incorrect amount, processed the payment late or more than once) the consumer can contest the error within 13 months and obtain appropriate compensation.

Fourth, PSD 1 has opened the market of payment systems, allowing entities other than banks (e.g. entrepreneurs and telecommunication entrepreneurs providing payment remittances) access to the payment service market. In order to protect consumers' money, these new institutions have become subject to regulation (supervision).

---

[2] The merchant, according to art. 2 point 1b of the PSA, is a recipient other than a consumer, to whom the settlement agent provides payment service.

[3] In Poland the PSA does not expressly prohibit (charges) surcharges.

1.2. Consumer Protection in PSD 2

PSD 2, which should be transposed into national law by 13 January 2018, on the one hand, has repeated the abovementioned instruments of protection in relation to the consumer, and, on the other hand, has introduced the following new regulations in respect to PSD 1:

1) the introduction of new payment services and new types of payment service providers resulting in increased competitiveness for the benefit of consumers;

2) new exceptions in the application of PSD 2 (which clarify the existing exemptions and grants control to national supervisory authorities over entities claiming these exclusions);

3) the prohibition of surcharges when using payment cards with a regulated level of interchange fees[4];

4) lowering the level of responsibility borne by the payment service provider, from EUR 150 to EUR 50, in the case of an unauthorised payment transaction[5];

5) increasing consumer protection in cases of card-based payment transactions where the exact transaction amount is not known at the time the payer gives consent to execute the payment transaction, for example when at automatic fueling stations, when signing car rental contracts or when making hotel reservations[6];

6) the obligation to introduce a method of accurate verification of the authorised consumer (payer).

The selected new instruments which provide legal protection to consumers introduced by PSD 2 are the subject of this article.

It is worth noting that consumer protection in the payment market is also regulated in Poland by the Consumer Rights Act[7]. Nevertheless, the application of this regulation is limited due to the provisions included in art. 4 paragraph 2 of the Consumer Rights Act[8].

---

[4] Regulation of the European Parliament and of the Council (EU) 2015/751 of 29 April 2015 on interchange fees for card-based transactions (Journal of Laws of the European Union of 19 May 2015), http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32015R0751&from=EN. Cf. more (Byrski, Sytniewski & Marcinkowska 2015).

[5] See the official press reports: http://europa.eu/rapid/press-release_MEMO-15-5793_en.htm.

[6] Recital 75 of PSD 2. The payer's payment service provider should be able to block funds on the payer's payment account only if the payer has given consent for the exact amount of the funds to be blocked.

[7] The Act of 30 May 2014, Consumer Rights (i.e. Journal of Laws of 2017, item 683, as amended).

[8] The regulation stipulates that provisions of the act shall not apply to agreements for payment services, except distance contracts.

2. The Term "Consumer" and "Payment Service Provider" and the Capital Requirements in Respect of the Providers, as a Part of Consumer Protection

2.1. The Term "Consumer" in Payment Service Act and PSD 2

In accordance with art. 4 point 20 of PSD 2, "consumer" means a natural person who is acting in payment service contracts for purposes other than his or her trade, business or profession[9].

Recital 53 of PSD 2 states that because consumers' and businesses' (enterprise') circumstances differ, they do not need the same level of protection. While it is important to guarantee consumers' rights by unwaivable provisions in a contract, it is reasonable to let enterprises and organisations make other arrangements provided they are not dealing with consumers. Member States should be, nevertheless, able to introduce a provision[10], under which micro-enterprises, as defined in Commission Recommendation 2003/361/EC[11], are treated in the same way as consumers[12].

The Polish legislature did not introduce an extended definition of what was considered a "consumer" in the Payment Services Act[13]. Hence, for the purposes of said Act, the definition of "consumer" should be understood as defined in art. 22 [1] of the Civil Code[14] – the "consumer" shall be understood as a natural person performing an act in law not directly related to his business or professional activity.

2.2. The Term "Payment Service Provider" in the Payment Service Act and PSD 2

Payment services are defined in the closed catalogue provided for in art. 3 paragraph 1 point 1–7 of PSA[15]. However, the Payment Services Act itself does not contain a definition of the term "payment service". The literature indicates

---

[9] Similarly, art. 4 point 11 of PSD 1.

[10] PSD 1 provided for the possibility for the Member States to apply the rules protecting consumers also in respect to micro-enterprises (art. 30 paragraph 2 and art. 51 paragraph 3 of PSD 1).

[11] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (Text with EEA relevance) (notified under document number C(2003) 1422), http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32003H0361.

[12] Similarly, recital 20 of PSD 1.

[13] The Payment Service Act of 19 September 2011 (i.e., Journal of Laws of 2016, item 1997, as amended), hereinafter: PSA.

[14] The Act of 23 April 1964 Civil Code (i.e., Journal of Laws of 2016, item 380, as amended).

[15] The enumeration is modelled on the annex to the PSD 1.

that there are approved financial services that constitute payment services and unapproved services and activities which, despite having features of payment services, are not considered as such, and, therefore, entities providing them will not be considered payment service providers.

The first of the above payment services described is the service of operating a payment account for the purpose of receiving cash deposits and making cash withdrawals from a payment account, and for any action necessary for maintaining such an account. Payment services also cover activities related to the transfer of funds into the payment account at the user's provider or at a different provider, so that this service can be conducted by executing direct debits, including one-off direct debits, or through the use of a payment card or a similar payment instrument or by providing transfer orders services, including standing orders.

Another payment service described is the performing of payment transactions, including an amount of cash made available to the user on credit[16]. The issuing of payment instruments, including credit cards, is also considered a payment service (Korus 2012, p. 29)[17].

An acquiring service is a payment service provided by settlement agents[18], which consists of enabling the execution of payment transactions by a merchant or through the latter, by means of the payer's payment instrument (e.g. by a credit card), in particular, consisting of handling the authentication, transferring to the issuer of the payment card or payment systems the payment orders of the payer or a merchant, in order to provide the merchant with the funds due to him, with the exception of activities involving the clearing and settlement within the framework of the payment system under the act on settlement finality.

Money remittances constitute another payment service, one which makes it possible to transfer money directly to the recipient or to a payment service provider that receives the funds for the recipient; after the transfer, funds are available to the recipient. Such remittance services transfer to the recipient, or to another provider that receives the funds for the recipient, cash received from the payer or of receiving the funds for the recipient and of making them available to the recipient. This service can be rendered by the offices of payment services[19].

---

[16] And in case of a payment institution or an electronic money institution, a short-term loan.

[17] Payment instrument, in accordance with art. 2 point 10 of the PSA, shall be understood as "a personalised device or the set of procedures agreed by the user and the provider, used by the user to make a payment order".

[18] According to art. 2 point 1a of the PSA, the settlement agent shall mean a provider established in the provision of payment services as referred to in art. 3 paragraph 1 point 5 of the PSA.

[19] Cf. more broadly (Zalcewicz & Bajor 2016, p. 95). Money remittance service is rendered without operating a payment account for the payer.

The last payment service is a service performed only with the use of ICT. It involves the execution of payment transactions where the consent of the payer to execute a transaction is provided using a telecommunication, digital or IT device and the payment is transferred to the provider of telecommunication, digital or IT services, acting only as an intermediary between the user commissioning the payment transaction and the recipient[20].

The activity related to the provision of payment services may be, in accordance with art. 4 paragraph 1 of PSA, carried out exclusively by payment service providers[21]. Moreover, payment institutions (and other payment service providers) are obliged to have holdings of initial capital set by law[22]. These regulations may be understood as an additional consumer protection because PSD 1 and PSD 2 are fully harmonised directives and all Member States shall write similar provisions into their domestic law systems[23].

---

[20] PSD 2 eliminated this payment service (there will apply general regulations concerning payment services), introducing, in turn, the exclusion to the payment transactions carried out by the provider of the network or electronic communications services, provided – alongside electronic communications services – for networks or services subscriber: (i) 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; or (ii) 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; provided that the value of any single payment transaction referred to in points (i) and (ii) does not exceed EUR 50 and: – the cumulative value of payment transactions for an individual subscriber does not exceed EUR 300 per month, or – 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 (art. 3 point l of PSD 2).

[21] The provider may only be: 1) a domestic bank, within the meaning of art. 4 paragraph 1 point 1 of the Act on Banking Law (The Act of 29 August 1997 on Banking Law (i.e. Journal of Laws of 2015, item 128, as amended), hereinafter: Banking Law); 2) a branch of a foreign bank, within the meaning of art. 4 paragraph 1 point 20 of the Banking Law; 3) a credit institution within the meaning of art. 4 paragraph 1 point 17 of the Banking Law and, accordingly, the branch of a credit institution within the meaning of art. 4 paragraph 1 point 18 of the Banking Law; 4) an electronic money institution; 5) a branch of the provider of postal payment services, rendering services in the Member State other than Poland, in accordance with the law of that Member State, authorised under the law of that Member State to the provision of payment services and the Polish Post Joint Stock Company (Poczta Polska Spółka Akcyjna) – to the extent to which separate provisions authorise it to provide payment services; 6) payment institution; 7) the European Central Bank, the Polish National Bank, and the central bank of another Member State – when not acting as monetary authority or public administration bodies; 8) a public authority; 9) the cooperative savings and credit union or the National Cooperative Savings and Credit Union within the meaning of the Act on Cooperative Savings and Credit Unions – to the extent to which separate provisions authorise them to provide payment services, 10) payment services office. Cf. more broadly (Grabowski 2012, p. 44).

[22] The amount of initial capital is regulated by art. 7 of PSD 2.

[23] Art. 107 of PSD 2.

In the course of completing legislative work on PSD 2, the continuous development of the types of payment services was pointed out. These include the emergence of the service of payment initiation or the services that allow access to a payment account held by the payment service provider[24]; is being provided by so-called Third Party Services Providers (TPP).

Currently, among the EU supervisory authorities and courts, there is no unified position on the legality of such services. Divergent interpretations are mainly due to the risk of the service provider acquiring data access to a payment account (e.g. username and password to e-banking), in violation of the agreement between the payer and the bank and in violation of certain legal provisions (e.g. in Poland – art. 42 paragraph 2 of PSA).

It must be stressed, however, that the European Central Bank (ECB), on the basis of PSD 1, consents to the provision of "payment account access services" and "payment initiation services". The ECB indicates in PSD 1 that "From a European perspective, payment account access services are rapidly gaining importance and payment initiation services are already among the most important payment methods for e-commerce in some Member States (…) The recommendations should not be interpreted as a warning against established TPPs in Europe. TPPs fill a gap by providing efficient and customer-convenient e-commerce services"[25]. On the another hand, accordingly, in its judgment of 20 July 2014, the Dutch court for Midden-Nederland, in the case ING Bank N.V. v. AFAS Software BV stated that AFAS acted unlawfully by asking clients on their website to provide access data to their bank accounts.

PSD 2 introduces these two new payment services and in the transitional provisions prohibits the introduction of the restrictions until the regulations of PSD 2 have been implemented into national law[26].

---

[24] Commission Staff Working Document {SWD(2013) 289 final} Annex 4: Background on market actors and payment methods Main actors in the market; source: http://ec.europa.eu/internal_market/payments/docs/framework/130724_impact-assessment-full-text_en.pdf (accessed: 31.12.2017).

[25] *Final Recommendations for the Security of Payment Account Access Services Following the Public Consultation*, https://www.ecb.europa.eu/pub/pdf/other/pubconsultationoutcome201405securitypaymentaccountaccessservicesen.pdf (accessed: 31.12.2017), pp. 3 and 5.

[26] On November 18, 2013 the Financial Supervision Authority, on its website, published a "Warning against allowing brokers access to bank accounts in online payments" (http://www.knf.gov.pl/Images/KNF_podawanie_danych_dostepu_do_rachunku_18_11_2013_tcm75-36300.pdf) (accessed: 31.12.2017), in connection with the identified practice of banks disclosing customers logins and passwords to entities other than their banks which maintain their accounts. On 14 July 2014 the Financial Supervision Authority published on its website the information "The risk associated with providing the login details to bank account to another bank" (https://www.knf.gov.pl/knf/pl/komponenty/img/KNF_podawanie_danych_dostepu_do_rachunku_18_11_2013_36300.pdf) (accessed: 31.12.2017). Both of these publications indicate the prohibition of customers disclosing data.

3. The Requirement of Strong Authentication of Transactions and the Principle of the Provider's Liability for Unauthorised Transactions as Elements of Consumer Protection

3.1. Strong Consumer Authentication

One of the basic goals of PSD 2 is to increase the level of consumer protection, particularly in the area of electronic payments. As indicated by recital 7 of PSD 2: "In recent years, the security risks relating to electronic payments have increased. This is due to the growing technical complexity of electronic payments, the continuously growing volumes of electronic payments worldwide and emerging types of payment services. Safe and secure payment services constitute a vital condition for a well-functioning payment services market. Users of payment services should therefore be adequately protected against such risks".

Such a goal is reflected in, among others, PSD 2 provisions in respect of strong authentication and in the light of a broadened scope of responsibility on the part of the payment service providers for unauthorised payment transactions. The implemented regulations are, in practical terms, one of the most significant changes posed by PSD 2 for payment service providers in the field of consumer protection[27].

3.2. Consumer Authentication in PSD 1 and the Payment Services Act

In the European legal order, following the provisions of PSD 1 and the Payment Services Act that implements it, the responsibility for unauthorised payment transactions (i.e. those to which the user did not consent – e.g. payment transactions made using data stolen by malware) is in principle borne by the payment service provider (e.g. the bank). The user is responsible for unauthorised payment transactions in exceptional cases, in particular, when he neglects the obligations set forth in the framework agreement regarding the security of the payment instrument and the protection of the "security" of this instrument (passwords, PIN codes). The consumer (payer) should also take adequate care associated with their use but within the limits required for the "normal" reasonable payer. According to recital 72 of PSD 2, "in order to assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all of the circumstances. The evidence and degree of alleged negligence should generally be evaluated according to national law".

However, while the concept of negligence arises from the failure to act with due diligence, gross negligence should be considered as more than mere negligence

[27] In terms of the relationship between payment service providers with the entrepreneur, these regulations may, in principle, be excluded in the framework agreement.

and should refer to a procedure in which there was a significantly higher degree of negligence on the part of the user; for example, when storing credentials used to authorise the payment transaction in the vicinity of a payment instrument, in an explicit form easily recognisable to third parties. Contractual terms and conditions relating to the provision and use of a payment instrument, the effect of which would be to increase the burden of proof that rests on the consumer or to reduce the burden of proof that rests on the issuer, should be considered null and void. Moreover, in specific situations, in particular where the payment instrument is not available at the point of sale, as is the case with online payment, it should be noted that the burden of proof of submitting evidence of alleged negligence lies with the payment service provider because in such cases the payer has very limited means to do so.

Basically, the payment service provider is, in principle, burdened with the obligation to equip the payment instrument, e.g. electronic banking services with the appropriate mechanisms to ensure the security of transactions (i.e. to ensure that they can only be made when authorised – namely when the payer gives his or her consent). The bank must prove that the payment transaction was authenticated by the user (art. 45 of PSA). This solution is pro-consumer.

PSD 2 maintains the above principle of the responsibility of the payment service provider for unauthorised payment transactions, and additionally reduces the limit from EUR 150 to EUR 50. Moreover, the current provisions impose on payment service providers the obligation to properly secure cash deposits and credentials. These obligations stem from the Payment Services Act and, when the payment service provider is a bank, additionally from provisions set down in the Banking Law.

The duty to provide security for the payers' credentials and cash has been further specified at the recommendation of the Financial Supervision Authority[28] on the security of online transactions (implementation of the guidelines of SecuRePay[29] and the European Banking Authority[30]). Recommendations have been issued

[28] Recommendation concerning the security of payment transactions performed online by banks, national payment institutions, electronic money institutions, national and cooperative savings and credit unions of 17 November 2015, issued by the Financial Supervision Authority, https://www.knf.gov.pl/knf/pl/komponenty/img/REKOMENDACJA_dot_bezpieczenstwa_transakcji_platniczych_43526.pdf (accessed: 31.12.2017).

[29] Recommendations for safety of online payment of 31 January 2013, issued by the European Forum for Security of Retail Payments (SecuRePay – European Forum on the Security of Retail Payments), https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpayment-soutcomeofpcfinalversionafterpc201301en.pdf (accessed: 31.12.2017).

[30] Final guidelines on the security of online payments of 19 December 2014, issued by the European Banking Authority (hereinafter: EBA), https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+%28Guidelines+on+the+security+of+internet+payments%29_Rev1 (accessed: 31.12.2017).

pursuant to art. 137 section 5 of the Banking Law[31], art. 102 paragraph 2 of PSA and art. 62 paragraph 2 of the Act on Cooperative Savings and Credit Unions[32].

The vast majority of the doctrine states that the Financial Supervision Authority is a body authorised to enact internal law by means of resolutions, in particular with regard to the recommendations set forth in banking law (Bączyk 2000, pp. 30–32; Fedorowicz 2013, p. 38; Tupin 1998, pp. 8–9; Kawulski 2013, pp. 573–574). The argument in favour of the organisational subordination of banks to the Financial Supervision Authority is perceived to be a functional relationship. Although banks and other financial institutions are entities essentially independent of the Financial Supervision Authority, what bonds them together is that the supervisory authority has extensive powers to influence their legal status.

The Constitutional Court held that the criterion of "organisational subordination", the fulfillment of which conditions the admissibility of the enactment of the internal law, must be understood more broadly than "hierarchical subordination" in the sense adopted in administrative law[33]. In addition, it is further argued that it is reasonable that the supervisory authority constituted "the implementing provisions" because it has the knowledge and professional competence to determine the content of the regulations that bind the supervised entities[34].

The recommendations of the Financial Supervision Authority are directed at the activities of banks, national payment institutions, national electronic money institutions and cooperative saving and credit unions. They oblige the application of so-called strong authentication for online transactions, yet this does not include mobile transactions and payments made via telephone, voice mail and SMS

---

[31] On 1 November 2015 the Banking Law stripped the Financial Supervision Authority of the authority to issue resolutions other than recommendations. Up to 31 October 2015, the Financial Supervision Authority issued resolutions on the basis of, among others, Banking Law (art. 9f, 9g, art. 71 paragraphs 4–5 and 8, art. 92b paragraph 3, art. 127 paragraph 5, art. 128 paragraph 6 point 3, art. 128 paragraph 8, art. 137 point 1a), which have since been replaced by the statutory delegation to issue regulations by the minister responsible for financial institutions. Currently, pursuant to art. 137 paragraph 1 point 5 of the Banking Law, the Financial Supervision Authority may issue recommendations on best practices of prudent and stable management of banks. The Financial Supervision Authority still has the power to issue resolutions which do not constitute recommendations based on the Act on Mortgage Bonds and Mortgage Banks (art. 11 and art. 24 paragraph 6) and the Act on Trading in Financial Instruments (art. 74 paragraph 8, art. 81g paragraph 5).

[32] Act of 5 November 2009 on Cooperative Savings and Credit Unions (Journal of Laws of 2013, item 1450 as amended).

[33] This view is still valid despite the repeal in the Banking Law of the power to issue resolutions by the Financial Supervision Authority, because this power has been left in other statutes regulating the financial market. Similarly, as it seems, P. Wajda (2009).

[34] Currently, the power to issue regulations by the minister responsible for financial institutions in many cases is manifested after the consultations with the Financial Supervision Authority.

technology. From their perspective, strong authentication is a procedure with the use of two or more of the following items classified as:

a) knowledge – something that only the user knows (the element of user's knowledge/user's memory, e.g. a static password, PIN),

b) possession – something that only the user has (equipment/device held by the user, e.g. a token/code generator, smart card, mobile phone), and

c) customer feature (a specific individual feature characteristic of the user, for example, a biometric characteristic such as a fingerprint).

In addition, the selected items must be mutually independent in the sense that a breach of security of one does not violate another (the other). At least one of the elements should be impossible to reuse and recreate (except for the characteristics of the client), and also be unsusceptible to undisclosed and unauthorised interception via the Internet. Moreover, the procedure of strong authentication should be designed in a manner that protects the confidentiality of credentials.

These recommendations impose on payment service providers a number of additional obligations designed to improve the safety of users of internet banking including consumers. These obligations include:

– a regular review of security policies of online payment services,

– carrying out a detailed evaluation of the risks regarding the safety of online payments and services related to these payments before they are implemented, and regularly after their implementation,

– the introduction of rules governing monitoring and procedures in case of security incidents,

– the use of adequate security measures,

– raising customer awareness about safely using Internet payment services, the burden of which has been shifted onto the payment service providers, including banks.

The obligation of applying the mechanism of strong authentication resulting from the recommendations is not absolute, due to the principle of "comply or explain" that has been adopted. It is therefore possible to waive the application of the recommendations of the Financial Supervision Authority and explain the reasons for non-compliance.

This state of affairs will change after the implementation of PSD 2, which imposes on payment service providers an obligation to use a strong authentication mechanism when the payer:

a) gains access to his or her payment account online,

b) initiates an electronic payment transaction,

c) carries out the operation using a remote channel, which may involve a risk of payment fraud or other abuses.

3.3. Strong Consumer Authentication in PSD 2

When establishing a new framework for the provision of payment services in the European Union, the EU legislature took the position that the existing protection offered to the consumer-payment service user was insufficient. This is mainly because most of the commonly used payment instruments are currently based on new technologies, and, moreover, these tools operate in an online environment (mobile applications, e-banking) or they are based on remote access (e.g. telephone banking). The increase in convenience for the consumer due to the use of Internet/remote payment instruments is, nevertheless, accompanied by higher risks.

PSD 2 extends the obligation to use the strong authentication mechanism on such operations as:

– initiating electronic payment transactions online – which also includes payment transactions using mobile applications that are excluded from the recommendations of the Financial Supervision Authority;

– carrying out operations using a remote channel (e.g. telephone, SMS, electronic channels – without the parties being physically present) that may pose a risk of payment fraud or other abuse, which are excluded from the recommendations of the Financial Supervision Authority.

In contrast to the applicable regulations (the Payment Services Act and recommendations of the Financial Supervision Authority), PSD 2 also details a more regulatory technical standard for mechanisms of strong authentication, which will be required from payment service providers. According to art. 98 of PSD 2, the proper body to develop regulatory technical standards (RTS) is the European Banking Authority (EBA), in cooperation with the European Central Bank. The regulatory technical standards should be developed by 13 January 2017 in consultation with the relevant stakeholders, including actors from the payment services market. In addition, these standards should be regularly reviewed. Currently, the regulatory technical standards are still in development and under consultation. The last consultation paper of 12 August 2016 is available on the website of the European Banking Authority[35]. The consultations proceeded until 12 October 2016. Final regulatory technical standards should be issued concerning the method of strong authentication.

The introduction of PSD 2 and its implementation in the future will not affect the validity of the recommendations of the Financial Supervision Authority. Payment service providers will still be bound by them, unless they are repealed

[35] https://www.eba.europa.eu/documents/10180/1548183/Consultation+Paper+on+draft++RTS+on+SCA+and+CSC+%28EBA-CP-2016-11%29.pdf/679054cf-474d-443c-9ca6-c60d56246bd1 (accessed: 31.12.2017).

due to the EBA adopting the RTS. In this context, it should be noted that PSD 2 differs from the recommendations of the Financial Supervision Authority: It does not impose on payment service providers the obligation that at least one of the elements used for strong authentication should not be possible to reuse and recreate (except for the characteristics of the client). Moreover, during the authentication, there is no reason that these elements cannot be disclosed and acquired without authentication via the Internet and should also be impossible to an undisclosed and unauthorised acquisition via the Internet[36]. Therefore, the requirements resulting from the recommendations of the Financial Supervision Authority and PSD 2 do not overlap in every aspect. The recipients of the standards contained in PSD 2 and in the recommendations of the Financial Supervision Authority should, therefore, take particular care to ensure the content of these two regulations are in line with each other, when preparing to implement strong authentication mechanisms.

After the adoption of regulatory technical standards it would be desirable, *de lege ferenda*, to repeal the recommendation of the Financial Supervision Authority, so that the Polish payment service providers are not forced to comply with a number of overlapping, but not always consistent regulations. The regulatory technical standards should, in fact, in the light of PSD 2, set a uniform level of technical standards for strong authentication throughout the entire European Union.

4. The Prohibition to Exclude or Limit the Liability of the Payment Service Provider who Uses Outsourcing for Damage Caused to the Consumer

4.1. The Prohibition to Exclude or Limit the Liability in Outsourcing in the Payment Services Act

Under the Polish legislation, art. 18 paragraph 2 of PSD 1 (currently art. 20 paragraph 2 of PSD 2) was implemented in art. 88 paragraph 1 and 2 of the PSA[37], according to which the national payment institution in the provision of payment services and in carrying out business activity of issuing electronic money shall be liable to users or holders of electronic money for the actions of its agents and other entrepreneurs, through which it provides payment services or makes redemption of electronic money, and for the entities performing operations on the

[36] Cf. the definition of strong authentication contained in the recommendations of the Financial Supervision Authority.

[37] Art. 84–90 of PSA shall apply to offices of service providers that can provide payment services through an agent and delegate to another entrepreneur the performance of specific operational activities related to the provision of payment services (art. 121 of PSA).

basis of the agreement referred to in art. 86 paragraph 1, as for its own actions. This liability cannot be excluded or limited, unless the liability for a failure or improper execution of a payment transaction is excluded in case of force majeure or if the failure or improper performance of a payment order is due to other legal provisions. The payer's payment service provider should assume liability for a correct payment execution, including, in particular, liability for the full amount of the payment transaction and for the time of the execution, as well as full liability for any failure (act or omission) of outsourcing partners at the subsequent stages of the payment chain up to the recipient's account.

If the account of the recipient's payment service provider is not credited with the full amount or if the full amount credited is delayed, the payment service provider of the payer should correct the payment transaction or, without undue delay, refund to the payer (including the consumer) the appropriate amount of the transaction. The payment service provider cannot exclude or limit this liability in relation to the payment services user, including the consumer.

4.2. The Prohibition to Exclude Liability in Outsourcing in PSD 2

In accordance with art. 20 paragraph 2 of PSD 2, "Member States shall require that payment institutions remain fully liable for any acts of their employees, or any agent, branch or entity to which activities are outsourced"[38]. This principle of liability applies whether the client is a consumer or an an entrepreneur.

PSD 2 explicitly states that it only applies to the contractual division of liability between the payment service user and the payment service provider, yet it also indicates that the payment service provider that does not bear liability will receive compensation for losses incurred or sums paid under the provisions concerning liability[39]. It seems that on this basis, the Polish legislature has introduced in art. 88 paragraph 3 of PSA a commitment that the liability of an agent and other entrepreneurs cannot be excluded or limited, through which the national payment institution provides payment services as well as the liability of the entity performing operational activities under the agreement referred to in art. 86 paragraph 1, vis-à-vis the national payment institution for the damage caused to the user as a result of non-performance or improper performance of the agreement referred to in art. 84 paragraph 2, or the agreement referred to in art. 86 paragraph 1.

---

[38] Similarly, PSD 1 in art. 18 paragraph 2, "Member States shall require that payment institutions remain fully liable for any acts of their employees, or any agent, branch or entity to which activities are outsourced".

[39] Recital 87 of PSD 2, as well as recital 47 of PSD 1.

Thus, any modification of unlimited liability of the outsourcing partner vis-à-vis the payment service provider for damage caused to the users (including consumers) is not permitted. It seems that such wording of art. 88 paragraph 3 of the PSA goes too far for two reasons. First, it prevents any restriction of the upper limit of the liability of the outsourcing partner, or the exclusion of the liability for ceased profits (*lucrum cessans*). Further, recital 87 of PSD 2 *in fine* states that further entitlements – except for losses suffered or sums paid – relating to recourse claims and the details of their content and the manner of pursuing them in connection with an improperly provided payment transaction should be the subject of consultation. These consultations shall take place between the outsourcing partner and the payment institution, and, thus, cannot be imposed by mandatory provisions[40]. Second, art. 92 paragraph 1 of PSD 2 relating to the right of recourse restricts this exclusion to cases where an unauthorised transaction took place within the definitions of art. 73 of PSD 2 or the transaction was not performed or an improper or delayed payment transaction took place, but not in all cases when using the services of subcontractors. There are also cases when the services of outsourcing partners are used concerning, for example, the services of contractual storage of archival data, whose improper performance does not affect the performance or a proper payment transaction, or its delay.

4.3. De lege ferenda Call in the Framework of Implementing PSD 2

In summary, there should be a *de lege ferenda* call in the framework of implementing PSD 2, to amend art. 88 paragraph 3 of the PSA, in order to reduce the instances of prohibiting the exclusion or limitation of the liability of the outsourcing partner in respect of the payment institution, on the one hand, only for the losses incurred or the sums paid by this institution, and, on the other hand, only to the actions/omissions of the outsourcing partner involved in the payment transaction. Such a change to art. 88 paragraph 3 of the PSA has no bearing on the legal position of consumers (the users of payment services), in relation to whom the payment institution always accepts unlimited liability for the acts or omissions of an outsourcing partner.

5. Conclusions

The European Union legislature, when establishing a new framework for the provision of payment services in the European Union (PSD 2), concluded that the existing protection for the consumer, the user of payment services, was

[40] Cf. more broadly the arguments in favour of such a possibility (Byrski 2015, pp. 113–124).

insufficient. It therefore decided to take three measures: First, to maintain the principle that the payment service provider was liable for unauthorised transactions but with a reduction in the amount of the liability from EUR 150 to EUR 50. Second, it introduced a ban on surcharges on payment cards with a regulated level of interchange fees. Third, it introduced the restriction that the payer's payment service provider would be able to block funds on the payer's payment account only if the payer has consented – using a method of strong consumer authentication – to have an exact amount of funds blocked.

Regarding the provisions concerning the prohibition of excluding or limiting the liability of an outsourcing partner in relation to the payment service provider, this ban should be limited only to losses incurred or the sums paid by the provider and only to the actions/omissions of the outsourcing partner involved in the payment transaction. This change to the Payment Service Act would not affect the legal position of the consumer (payment service user), in relation to whom the payment service provider always accepts unlimited liability for the acts or the omissions of an outsourcing partner.

Bibliography

Bączyk M. (2000), *Zarys prawa bankowego. Część I. Prawo systemu bankowego* [An outline of the banking law. Part I. The law of the banking system], TNOiK, Toruń.

Byrski J. (2015), *Ustawowy zakaz wyłączania lub ograniczania odpowiedzialności partnera outsourcingowego wobec banku* [The statutory ban on excluding or limiting the liability of an outsourcing partner in respect of the bank] (in:) A. Olejniczak, J. Haberko, A. Pyrzyńska, D. Sokołowska (eds), *Współczesne problemy prawa zobowiązań* [Contemporary issues of contract law], Wolters Kluwer, Warszawa.

Byrski J., Sytniewski L., Marcinkowska A. (2015), *Komentarz do rozporządzenia nr 2015/751 w sprawie opłat interchange w odniesieniu do transakcji płatniczych realizowanych w oparciu o kartę* [Commentary on Regulation No 2015/751 on interchange fees for card-based payment transactions], LEX/el.

Fedorowicz M. (2013), *Nadzór nad rynkiem finansowym Unii Europejskiej* [European Union financial market supervision], Difin, Warszawa.

Grabowski M. (2012), *Ustawa o usługach płatniczych. Komentarz* [Act on Payment Services. Commentary], C.H. Beck, Warszawa.

Kawulski A. (2013), *Prawo bankowe. Komentarz* [Banking Law. Commentary], Warszawa.

Korus K. (2012), *Pojęcie usługi płatniczej w ustawie o usługach płatniczych* [The concept of payment service in the Payment Services Act], "Monitor Prawa Bankowego", nos 7–8.

Pacek M. (2014), *Usługi płatnicze. Komentarz, art. 16* [Payment services. Commentary, art. 16], Lexis Nexis, Warszawa.

Tupin R. (1998), *Czy i w jakim trybie uchwały i zarządzenia Komisji Nadzoru Bankowego mogą być uznane za niezgodne z Konstytucją?* [Whether and in which procedure the resolutions and orders of the Banking Supervision Committee may be considered

inconsistent with the Constitution?], "Przegląd Ustawodawstwa Gospodarczego", nos 7–8.
Wajda P. (2009), *Rola decyzji administracyjnej w nadzorze nad polskim systemem finansowym* [The role of the administrative decision in the supervision of the Polish financial system], C.H. Beck, Warszawa.
Zalcewicz A., Bajor B. (2016), *Ustawa o usługach płatniczych. Komentarz* [Act on Payment Services. Commentary], Wolters Kluwer, Warszawa.

Ochrona konsumenta w drugiej dyrektywie w sprawie usług płatniczych (2015/2366/UE) – wybrane zagadnienia

(Streszczenie)

Dyrektywa 2007/64/WE w sprawie usług płatniczych (PSD 1) uregulowała kwestie ochrony konsumentów w zakresie usług płatniczych. W pierwszej kolejności należy wskazać, że konsument uprawniony został do otrzymywania wszelkich niezbędnych informacji przed wykonaniem konkretnej transakcji płatniczej, jak i po jej wykonaniu. Po drugie, konsument powinien zostać zaznajomiony z wszelkimi opłatami, które jest zobowiązany ponieść za płatności dokonywane w sklepach, w tym w sklepach internetowych. Po trzecie, PSD 1 zapewniła ochronę praw konsumentów w przypadku nieautoryzowanych lub nieprawidłowych opłat naliczanych na konsumenckim rachunku płatniczym. Po czwarte, w ramach PSD 1 nastąpiło otwarcie rynku usług płatniczych, co umożliwiło podmiotom innym niż banki świadczenie usług płatniczych. W celu należytej ochrony pieniędzy konsumentów przedmiotowe instytucje poddane zostały szczegółowej regulacji (nadzorowi).

Prawodawca unijny, ustanawiając nowe ramy świadczenia usług płatniczych w ramach Unii Europejskiej (PSD 2), doszedł jednak do wniosku, że istniejąca ochrona konsumenta – użytkownika usług płatniczych, jest niewystarczająca. Z tego też względu zdecydował się na wprowadzenie nowych instrumentów prawnych, których zadaniem jest wzmocnienie tej ochrony. Po dokładnym ich przeanalizowaniu wydaje się, że część z nich należy ocenić pozytywnie, niemniej w stosunku do pozostałych regulacji należy podnieść uwagi krytyczne.

Słowa kluczowe: dyrektywa PSD 1, dyrektywa PSD 2, usługi płatnicze, ochrona konsumenta usług płatniczych, silne uwierzytelnianie, silne uwierzytelnianie klienta.