Dariusz Gradzi

Third Party Providers (TPP)[1] – new payment service providers in the Internet and mobile environment. Review of legal regulations and analysis of possible threats to cybersecurity of the paying critical infrastructure

Introductory remarks

Payment Services Directive (PSD I)[2] has introduced the notion of payment services to the European legal order and the closed catalogue of those services, as well as providers of payment services (so-called suppliers). Since its entry into force on the market, new paying electronic services based on Internet infrastructure have developed, including in particular services based on access to payment accounts (including banking) by third parties, which such permission is granted to the holder (user) of the account (e.g. bank client).

Electronic payments distinguishes between Internet payments[3] (made via the Internet) and mobile payments[4]. They may be carried out, inter alia, by means of payment using a payment card and by transfer orders [traditional bank transfer or the so-called Pay-By-Link[5] (PBL). The development of trade in the Internet environment

[1] The so-called Third Party Payment Service Provider – Supplier of payment services being a third party. Cf. M. Mostowik, *Legal Protection of payment account information in the light of account information services (AIS)*, Monitor of Banking Law, July – August 2017, p. 32.

[2] *Directive 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,* Unit EU L 319/1 of 5 December 2007.

[3] B. Chinowski, *Electronic Payment methods. Essence, development, projections,* Electronic version: https://www.knf.gov.pl/knf/pl/komponenty/img/Elektroniczne%20metody%20platnosci.pdf P. 5 [access: 20 X 2017].

[4] These are payments made using the mobile equipped in the operating system, with a multimedia interface using radio technology, telecommunications networks WI-Fi(GSM, GPRS, UMTS, Wi-Fi, Nfc, Rfid, Bluetooth), Final Recommendations for the Security of Payment Account Access Services Following the Public Consultation, the European Central Bank https://www.ecb.europa.eu/pub/pdf/other/pubconsultationoutcome201405securitypaymentaccountaccessservicesen.pdf. [access: 25 X 2017].

[5] This is an Internet payment method that involves the fact that when shopping online, during the payment through the "payment gateway" the customer a special link that directs it to bank who runs his account and after logging in to the electronic banking system there is a supplemented format the transfer with the recipient's data (usually the billing agent) and the amount. After authorization the recipient gets a message about execution and can proceed to fulfill the contract, which significantly speeds up online transactions. The condition of the payer's use of this service is its sharing by the bank in which the payer has an account. Cf. M. Grabowski, *Payment Instruments in Polish law*, Warszawa 2013, https://depotuw.ceon.pl/bitstream/handle/item/327/Instrumenty%20Płatnicze%20w%20prawie%20polskim.pdf?sequence=1, p. 211 [access: 4 X 2017].

and the need to accelerate the execution of the payment process has led to the evolution of the initiating services by introducing an interface (so-called "Payment gateway", "Payment Gate") linking the merchant website (e.g. with the payment service provider's website (e.g. bank).[6] In addition to the payment services traditionally designed to make payments between the payer and the recipient of the funds (or the entity acting on the basis of the contract,e.g. a clearing agent), new complementary services have emerged, referred to in this article and which introduces the second directive on payment services (PSD II)[7]:

- third party payment initiation service,
- third party access to account information service,
- confirmation of availability of funds on payment account.[8]

The above services provide the user with the opportunity to expedite the payment transaction and aggregated[9] online information about the payment account, provided through the interface of the payment account provider. With this last service, you have the ability to quickly orient yourself to your financial situation.[10]

The object of this study will be the presentation of new payment services introduced to the European and the same Polish legal order by the PSD II Directive and micro and macro threats which may involve the functioning of new Payment services. The cornerstone of these rules in the PSD II directive is the granting of rights to the payers to use third party providers (TPP) and the need to respect this right by the payment account provider (including bank) – the so-called Account Servicing Payment Service Provider (ASPSP), as appropriate mechanisms are provided for the[11] legal which break with possible lack of willingness to cooperate by ASPSP of TPP.[12] For this reason, ASPSP were forced to work legally to cooperate with TPP. In current market realities ASPSP often prevent the development of TPP by: blocking specific IP addresses[13] or blocking the payer's bank account[14] and preventing the so-called Screen Scraping.[15]

---

[6] Cf. Recital 27 of the preamble to the PSD directive.

[7] *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, 2013/36/EU and Regulation (EU) 1093/2010 and repealing Directive 2007/64/EC*, Dz. Unit. EU L 337/35 of 23 December 2015.

[8] Unlike the Payment Initiation service and account information services, the process of confirming the availability of cash is not a separate payment service. Cf. K. Korus, *Access-based services in the PSD II directive*, Monitor Banking Law, July-August 2017, p. 85.

[9] It refers to all kinds of information regarding multiple-element sets of unitary objects or multiple-element sets of features of those objects. Cf. J. Oleński Ekonomika informacji. Podstawy, Warszawa 2011, p. 209.

[10] Theme 28 Recital Directive PSD II.

[11] Sanctions of the supervisory Authority – the KNF, the obligation to notify of Art. 68 paragraph 6 PSD II.

[12] Should be noted that the business terms of TPP are direct competition for ASPSP.

[13] Internet Protocol (IP), Cf. http://munitus.pl/co-to-jest-ip.html [access: 4 X 2017].

[14] Cf. M. Mostowik, *Legal Protection of payment account information in the light of account information Services (AIS)*, Monitor of Banking Law, July – August 2017, p. 33.

[15] Screen Scraping – The method of access to the user's online banking, whereby the client

Statistical and hazard data

The feature of common services TPP is the fact that in order to perform them is necessary to gain access by a third party (TPP) to a payment account (banking). The development of non-cash payments, including electronic due to continuous technological progress, has led to the emergence of new payment services in the form of services based on access by third parties to payment accounts (including banking). PSD II is not creating these services in the factual context, but merely trying to capture them in a regulatory aspect, because until now, although they have been operating on the financial market for many years, they have not been in a legal regulation. Services of this type have hitherto remained outside the regulatory area, because in their case there is no entry by TPP in possession of cash[16], which allowed them to benefit from the exclusion of the application of the PSD and the Payment Services Act (UUP)[17] in the wording before implementation to the Polish legal order PSD II.[18] PSD II has brought changes in the form of necessity – in principle – to obtain the authorization of the supervisory authority (in Poland – the Financial Supervision Commission) to provide these services.

The services of TPP are designed to facilitate and expedite the making of payments in the Internet environment. However, attention should be paid to the possible dangers that will entailed the emergence of new services and new suppliers in the context of the following statistics. Statistics show that the number of detected cyber attacks in Poland in 2015 in comparison with 2014 was increased by 46 percent. The biggest risk factor for the financial sector is the threat of attacks on IT systems.[19] In 2014, in Poland, approximately 230,000 computers had malicious software installed, of which 50,000 of cases were malicious software in the form Trojan Bank.[20] The number of mobile banking users over the last 4 years has risen to about 8.2 million (an increase of 680 percent).[21] In the same

authorizes the bank (e.g. in which the credit is applied) to log in to his payment account at another bank (where the user has the payment history) by means of log the first bank login data. Logging in by analysis banking interface content by the IT system First Bank, which automatically enter the Customer's login and password in the specified fields and login to the online banking system. Cf. The warning issued by the KNF 14.07.2014, "*Risks associated with giving another bank login data"*, https://www.knf.gov.pl/?articleId=53072&p_id=18 [access 23 X 2017].

[16] Art. 6 paragraph 10 UUP from ZW. with article 3. 3 (a) 1 PSD I.

[17] *Payment Services Act of 19 August 2011* (OJ no 199, item 1175, Subsequent. D.).

[18] *The act of financial service law of 10 May 2018 Amending the Payment Services Act and certain other provisions of the (OJ 2018, item 1075).*

[19] Information Technology, http://zasoby.open.agh.edu.pl/~08pdiakow/indexb0c5.html?q=node/37 [access: 4 X 2017].

[20] Cf. A. Marciniak, bank CERT – New weapons in the fight against cybercrime [in:] A. Kawiński, A. Sieradz (ed.), *Challenges of banking Informatics 2016*, Gdansk 2016, http://www.efcongress.com/sites/default/files/wyzwania_informatyki_bankowej_0.pdf, pp. 181–182 [access: 2 X 2017].

[21] Cf. Research reports conducted by the PRNews.pl portal In the fourth quarter of 2012 and I Quarter 2017, https://prnews.pl/raport-prnews-pl-rynek-bankowosci-mobilnej-i-kw-2017-360755

way, the number of owners of mobile banking smartphones in 2013 was 12 percent, whereas in 2015 already 43 percent.[22]

The number of non-cash transactions is increasing on average 15 percent year-to-year. The number of transfer orders increased from PLN 31 trillion in the year 2010 to 47.5 trillion ZL in the year 2015. The share of transfer orders in the year 2015 in general non-cash transactions amounted to 45 percent. In all non-cash transactions, the number of transactions with a credit card amounted to 54 percent in the year 2015, while in 2010 it was 36 percent. Card transactions in the years 2009-2015 reached on average a year increase of 24 per cent.[23] The number of payment cards issued in Poland in the year 2014 more than 36 million.[24] In 2013, the share of fraudulent card transactions in the value of all card transactions amounted to 0.005 percent.[25]

In parallel between 2005–2015, there has been a dynamic increase in the acceptability of payment cards (networks constituting the so-called POS points of sale – where payment by credit card is accepted) from 55 thousand POS points in 2005 to 184,000 in 2015. The number of single POS terminals to accept payment cards has increased during this period from 129,000 to 463,000. The percentage of Poles actively using the bank account over the Internet is also growing. In 2009 it was 46 percent, while in 2016, 69% percent.[26] Number of bank accounts held for private individuals by banks, branches of institutions and credit unions increased from 44 million in 2010 to 58 million in 2015.[27]

In the first quarter of 2017, more than 15,000 merchants were seen on the Internet[28] and 11.5 million payment transactions. The value of these transactions amounted to 1.78 billion. On average, more than 128 000 transactions were recorded.[29]

These statistics show the enormous and irreversible trend of the growth of non-cash payments and electronic payment transactions.[30]

[access: 23 X 2017]; https://prnews.pl/raport-prnews-pl-rynek-bankowosci-mobilnej-iv-kw-2013-16158 [access: 23 X 2017].

[22] Cf. A. Marciniak, Bank CERT – New weapon in the fight against cybercrime [in:] A. Kawiński, A. Sieradz (ed.), *Challenges of banking Informatics 2016*, Gdansk 2016, http://www. Efcongress. com/sites/default/files/wyzwania_informatyki_bankowej_0.pdf, p. 181-182 [access: 2 X 2017].

[23] *Status of cashless trading in Poland*, https://www.mr.gov.pl/media/30118/Rozwoj_obrotu_bezgotowkowego_112016.pdf [access: 10 X 2017].

[24] Comparison of selected elements of the Polish payment system with the systems of other European Union countries in 2015 https://www.nbp.pl/systemplatniczy/obrot_bezgotowkowy/porownanie_UE_2014.pdf, p. 18 [access: 10 X 2017].

[25] Ibid p. 31.

[26] D. Maison, *Attitude of boxes towards non-cash trading. Test report 2016 and comparative analysis with data from 2009 and 2013,* https://www.nbp.pl/badania/seminaria/8v2017.pdf [access: 10 X 2017].

[27] *Comparison of selected elements of the Polish payment system with the systems of other countries of the European Union for 2015*, https://www.nbp.pl/systemplatniczy/obrot_bezgotowkowy/porownanie_UE_2014.pdf, p. 6 [access: 10 X 2017].

[28] E.g. online store is which accepts.

[29] *Information on payment cards and quarter 2017*, https://www.nbp.pl/systemplatniczy/karty/q_01_2017.pdf, p. 36 [access: 10 X 2017].

[30] *Status of cashless trading in Poland*, https://www.mr.gov.pl/media/30118/Rozwoj_obrotu_

This data leads to the conclusion that the activities of TPP especially in the initial period should be particularly supervised and verified, given the potential risks to the financial ecosystem, which is based on the mutual trust of its participants and caring for the safety of end users.

Payment services and their suppliers-legal characteristics

Before further analysis, it is necessary to present deadlines which will help to understand the process of electronic payment and its participants. According to the Polish Payment Services Act (UUP):

- *Provider* – is a payment service provider. UUP contains a closed catalogue of suppliers, which may include national banks, credit institutions, electronic money institutions, payment institutions, credit unions or payment service bureaus, which means that other companies are not allowed to provide these services under penalty of criminal[31],
- *Merchant* – It is a recipient other than the consumer for whom the accounting agent provides a payment service (e.g. a shop or an online store). This is the entity that accepts the payment in a non-cash form[32],
- *Payment service* – It is a service whose essence is the change of ownership of funds, e.g. a bank transfer where funds from an account in one bank are credited to a user's account in another bank. This service therefore aims to allow the payer to transfer funds to the payee. UUP introduces a closed payment service catalogue,
- *User* – It is a natural person, legal entity or an organizational unit not being a legal person, which the law confers legal capacity, using payment services as payer or consignee,
- *Payer* – It is a natural person, legal entity or an organizational unit which is not a legal person, which the law confers a legal capacity to make a payment order leading to the debiting of its payment account or the payment of funds (the entity making payments),
- *Recipient* – it is a natural or legal person, or an organizational unit which is not a legal person, which the law confers the legal capacity of the recipient of the funds constituting the subject of the payment transaction (the entity receiving the payment),
- *Payment order* – This is a statement by the payer or payee to the supplier containing the command to execute the payment transaction.[33] It initiates a payment transaction. The payment instrument may be used for its assembly. The order must have data enabling the transaction to be carried

bezgotowkowego_112016.pdf [access: 10 X 2017].

[31] Art. 150 and N. UUP.

[32] M. Pacak, *Payment Services. Comment*, Warszawa 2014, LexisNexis p. 181.

[33] Ibidem, p. 182.

out, such as: payer and payee data, transaction amount, unique customer ID – e.g. IBAN-International Bank account number Account Number[34],

– *Payment transaction* – This is initiated by the payer or recipient of the deposit, transfer or withdrawal of funds. A payment transaction may be:
  • *Initiated by the payer* e.g. transfer order (traditional bank transfer), where the transaction order of the payer sends to his payment service provider[35],
  • *Initiated by the customer* – where the payer has previously given consent to initiate a transaction. In this case, the payee initiates a payment transaction without the payer's participation (e.g. direct debit[36]),
– *Payment Instrument* – this is the device or user-agreed and provider-set of procedures used by the user to place payment orders. These are the title of the example:
  • Technical procedures, such as electronic banking[37],
  • Material objects such as Payment cards – the so-called trading instruments[38],
– *Payment Card*[39] – This is a cash withdrawal card (ATM) or for making a payment order via merchant or a billing agent,
– *Debit Card* – A payment card enabling the execution of payment transactions, except for transactions in the weight of cash made available to the user for credit,
– *Credit card* – This is a payment card allowing the execution of payment transactions into the weight of the funds provided to the user for credit.

In the light of the UUP in the Polish legal order there are among others the following payment services:

- Payment Account maintenance (it should be noted that the payment account holder is not only banks), making cash withdrawals,
- Accepting cash deposits,
- Execution of payment transactions by means of a payment card or similar payment instrument,
- Execution of direct debit,
- Transfer command (traditional bank transfer),
- Issuance of payment instruments (e.g. payment cards), so-called Issuing,
- *Acquiring* execution of payment transactions initiated by the merchant or through the payer's payment instrument, in particular their authorization, sending to

[34] M. Grabowski, *Payment Services Act. Comment*, Warszawa 2012, C.H. Beck, p. 28.
[35] Ibidem, p. 27.
[36] Art. 63d Law of 29 August 1997 (OJ no 140, item 939).
[37] M. Grabowski, *Payment Services Act. Comment*, Warszawa 2012, C.H. Beck, p. 19.
[38] K. Korus, *Concept of payment service in the payment Services ACT*, Monitor of Banking Law, July-August 2012, p. 37.
[39] It should be noted that the subjects of payment cards are regulated particular by Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on levies on interchange with respect to card-based payment transactions.

the issuer of the payment card or payment systems for payment orders having to transfer to acceptor the funds owed to it.[40] Except for the settlement operations of the payment system within the meaning of *The Law on settlement finality in payment and securities settlement systems and the rules for the supervision of these systems*.[41] These are transactions in which, for example, a payment by credit card is made in the store (merchant), which authorizes and settles the transaction on the services acquiring provided by the paying agents, transmitting a payment order to the bank – the publisher of the card belonging to the person making the payment and then, after receiving from that bank the cash, settling with the acceptor,

- The provision of money remittance (transfer to the payee of the cash received from the payer without the payment account being carried out – e.g. the receipt of fees for small bills in the purpose of their transmission to service providers or the receipt of payments for their make),
- provision of a payment transaction initiation service,
- provision of account information Access Service.[42]

Areas of payment infrastructure exposed to risk

The following places must be distinguished.[43] In the area of electronic payment infrastructures exposed to threats. These are:

– Payment Systems[44], entities accounting for payment transactions (e.g. National Clearing House) and payment card systems infrastructure – payment schemes (card organizations)[45],
– IT banking systems[46] (and) the infrastructure of entities involved in the processing of payment transactions (suppliers, including clearing agents),
– Merchants infrastructure, i.e. recipients of an electronic payment[47],

[40] R. Kashubian, Ł. Obzejta, *Payment cards in Poland*, Warszawa 2012, Wolters Kluwer, p. 107.

[41] *The Act on settlement finality in payment and securities settlement systems and the rules for the supervision of these systems of 24 August 2001* (OJ no 123, item 1351, Subsequent D.).

[42] *Provision of services and initiation of payments and service access to account information has been added to UUP based on PSD II Act of 10 May 2018 amended the law on payment services and certain other acts (OJ 2018, item 1075).*

[43] D. Gradzi, *Electronic payment security as part of Cybersecurity States – Review of legal regulations*, Internal Security Review No. 16 (9) 2017, p. 38.

[44] SORBNET2, TARGET2-NBP, for large payment, ELIXIR, EXPRESS Elixir, National settlement system, payment system BlueCash, the BLIK mobile payment system, the card payment system for retail payments, http://www.nbp.pl/home.aspx?f=/systemplatniczy/nadzor_syst_platn/systEmy_platnosci. HTML [access: 15 X 2017].

[45] Article 2 (1) 19b *Payment Services Act of 19 August 2011* (OJ no 199, item 1175, Subsequent. D.), define a card organization as: an entity that defines the issuant and acceptance rules of a payment card, which includes contracts with publishers (banks) or billing agents (e.g. VISA or Mastercard).

[46] K. Radziejewski, *Cybersecurity Governmental administration in Republic of Poland*, Internal Security Review, No. 16 (9) 2017, p. 313.

[47] Article 2 (1) 1b *UUP* define merchant as a customer other than the consumer to whom the payment agent provides the paying service (including, for example, an online store that accepts

– Applications and infrastructure for end users, both online and mobile, including mobile devices and computers.

Part of the above elements is a critical infrastructure[48], which is covered by the National Programme for the Protection of Critical Infrastructure.[49] These elements should be classified as financial systems, the operation of which is possible on the basis of communication systems and ICT systems.

"Critical State Infrastructure" includes, inter alia, banking and financial systems and telecommunication.[50] It consists of real (objects, servers) and cyber systems which, in case of coexistence, allow the provision of payment services. Due to the specificity of the payment services (remote access) and the open nature of the banking systems that can be accessed using public networks, they are exposed to cybercrime. Cybercrime is understood as a *"The use of telecommunications networks to violate any legal good protected by criminal law"*.[51] Government Programme for the Protection of Cyberspace Republic of Poland for the period 2011–2016[52] defines "cybercrime" as "criminal offences committed in "cyberspace". „Cyberspace" is defined in the above document as "a digital space for the processing and exchange of information created by ICT systems and networks, together with their associated relationships and user relations". Statistics of incidents in cyberspace coordinated by CERT[53] show an increase in the number of incidents compared to previous years. In 2014, more than 12,000 entries were registered, of which 7.4 thousand qualified as actual incidents. In 2015, more than 16,000 entries were registered, and as actual incidents qualified 8.9 thousand cases.[54]

In addition, it should be given that the occurrence of a threat in the above areas of critical infrastructure may be classified as a terrorist event[55] imply introduction

---

both card payments and the so-called payment services. Pay-By-Links – Instant transfers, where the amount of the payment transaction is dealt with By an intermediate settlement agent).

[48] Within the meaning of art. 3 point 2 Point. b), c) and D) *The Crisis Management Act of 26 April 2007* (OJ no 89, item 590, Subsequent. D.).

[49] Within the meaning of art. 5b *The Crisis Management Act of 26 April 2007* (OJ no 89, item 590, Subsequent. D.).

[50] Cf. Art. 3 paragraph 2 *Act of 26 April 2007 on crisis management* (OJ no 89, item 590, Subsequent. D.) and R. Kośla, *Protection of critical infrastructure in Poland – Current state of work*, HTTP://WWW.CERT.PL/pdf/Kosla_p. PDF [access: 2 X 2017].

[51] M. Staszczyk, *Unauthorized banking transactions as a manifestation of cybercrime*, electronic version, http://www.finanseiprawofinansowe.uni.lodz.pl/Publikacje/5/4_Staszczyk.pdf, p. 46 [access: 2 X 2017].

[52] *The Government Programme for the Protection of cyberspace RP*, https://bip.mswia.gov.pl/bip/programy/19057,Rzadowy-Program-Ochrony-Cyberprzestrzeni-RP-na-lata-2011-2016.html [access: 17 VIII 2018].

[53] Government Incident Response Team, http://www.cert.gov.pl/cer/o-nas/15,O-nas.html [access: 10 X 2017).

[54] http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/910,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2015-roku.html [access: 3 X 2017].

[55] In the meaning of article 2, point 7 *Act of 10 June 2016 on anti-terrorist activities* (OJ 2016, item 904).

of CRP alarm steps[56] where there is a suspicion that the offence is caused by a terrorist offence or the threat of such a crime.[57] A terrorist offence is, inter alia, an offence which is punishable by a custodial sentence whose upper game is at least 5 years, committed in order to cause serious disturbance to the regime or economy of Republic of Poland the threat of committing such a prohibited act, which in particular concerns critical infrastructure. It is possible to use the banking critical infrastructure by TPP and cause damage to the banks, as well as their clients, whose height can not be predicted.

Third Party Providers (TPP) – legal regulations

The legal acts governing access by third parties (TPPs) for payment accounts are[58]:

- PSD II directive,
- Regulatory Technical Standard (RTS)[59] – Concerning the strong authentication of the client and universal and secure communication, regulating the way of communication between TPP, and ASPSP[60], issued pursuant to art. 98 paragraph. 4 ph. 2 PSD II in connection with article 3. 10-14 of Regulation (EU) No 1093/2010 of 24 November 2010 establishing a European supervisory authority (European Banking Authority). RTS does not require implementation in national legal order[61] and EU member states are to ensure that it is forcibly applied by TPP and ASPSP from the first day after 18 months from the date of entry into force of the RTS,
- UUP and the Act amending the Payment Services Act and certain other acts.[62]

[56] According to Article 15 (1) 2 *Act of 10 June 2016 on anti-terrorist activities* (OJ 2016, item 904).

[57] For the purposes of Article 115 Par. 20 of the Penal Code of 6 June 1997 (OJ no 88, item 553).

[58] Included in the elaboration of both legal acts enacted and the legislative phase.

[59] RTS are issued based on Art. 290 of the Treaty on Functioning of the EU (OJ C 202 (2016), and are called. Level in the system of EU legislation. They shall be drawn up by the European Banking Authority (EBA) – The European Banking Authority and as a project are submitted to the European Commission. The European Commission has the power to adopt the so-called Act Non-Legislative which complements the legislative act (in this example, the PSD II directive). The RTS is therefore binding on Member States or supervised institutions (e.g. banks). RTS the European Commission submits to the Council of the European Union and the European Parliament, which may reject the act, cf. *The structure and status of European Union legislation with a particular focus on RTS, ITS and the so-called. Guidelines*, http://mifid.pl/wp-content/uploads/2015/11/Struktura-aktów-Unii-Europejskiej-ze-szczególnym-uwzględnieniem-RTS-ITS-i-tzw.-Guidelines.pdf, p. 4 [access: 4 X 2017].

[60] https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2 [access: 14 X 2017].

[61] K. Korus, access-based services to the account in the PSD II directive, Monitor Banking Law, July-August 2017, p. 82.

[62] Cf. Act Amending the Payment Services Act and certain other provisions of 10 May 2017., http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001075 [access: 19 VI 2018].

The common scope of the PSD II directive to TPP

TPP are currently operating in the payment service market and are active participants carrying a huge volume of payment transactions both in terms of amount and quantity[63] (in 2014 of the services of one only provider of TPP used 8 million people in 11 countries, which supplier since 2005 has conducted over 100 million transactions). For this reason, PSD II introduced the requirement not to discriminate against these entities until the implementation of its provisions.[64] It is worth noting that the Financial Supervision Commission has in the past issued warnings before the activities of TPP.[65]

The PSD II introduces three types of services for TPP, also referred to as services XS2A.[66] They are:

- Payment Initiation Service (Payment Initiation Service-PIS): It means a service which consists in initiating a payment order from a user at the request of a payment account held with another payment service provider.[67] The PIS may not at any time be in possession of cash, which distinguishes this form of payment from the so-called Instant Transfers (Pay-by-Link), where the "broker" – the clearing agent shall be in possession of these resources,
- Account Information Access Service (Account Information Service – AIS): means an online service that consists of providing consolidated information about a payment account held by a payment service user[68],
- Confirmation of the availability of funds on the payment account (Confirmation of the Availability Of Funds -CAF). The CAF does not constitute a separate payment service and is not listed in annex 1 of the PSD II directive.

ASPSP is obliged to allow PIS and AIS to rely on user authentication procedures provided by ASPSP.[69] This regulation leads to the conclusion that TPP has the right to use its own authentication of the user, independent of ASPSP authentication, but may also rely solely on the authentication of the user used by ASPSP.

---

[63] https://www.sofort.com/pol-PL/newsroom/prasowe/SOFORT-Banking-utrzmuje-szybie-teo-wzrotu[access23X2017].https://retailnet.pl/2015/06/22/13453-dagmara-kruszewska-sofort-3-ml-tra-mieieczie/, http://prnews.pl/wiadomosci/sofort-wyniki-za-1-polowe-2016-50-sklepow-dzieie-chce-rozac-wspolrae-6553123.html [access: 14 X 2017].

[64] Recitals 29 and 33 to the PSD II directive.

[65] *A warning of the KNF by admission of intermediaries to a bank account in Internet payments of 18.11.2013, the risk of giving another bank login data for the 14.07.2014*, Cit. For: "*Recommendations concerning the security of payment transactions performed in the Internet by banks, national payment institutions, national e-money institutions and credit unions* Issued by the KNF in November 2015, p. 2, https://www.knf.gov.pl/dla_rynku/regulacje_i_praktyka/rekomendacje_i_wytyczne/Rekomendacja_dot_bezpieczenstwa_transakcji_platniczych [access: 25 X 2017].

[66] So-called. Access This Account (Account Access), Cf. M. Mostowik, *Legal Protection of payment account information in the light of account information Services (AIS)*, Monitor of Banking Law, July – August 2017, p. 32.

[67] Art. 4 paragraph 15 of PSD II.

[68] Art. 4 point 16 PSD II.

[69] Art. 97 paragraph. 5 PSD II.

All the legal obligations imposed by PSD II on ASPSP apply only if they lead a payment account for the user. The bank account is then a payment account when it is used for the execution of payment transactions.[70] Access to information and functionality other than a payment account (e.g. credits, deposits, deposits, investments) is not regulated by the PSD II directive.[71]

The scope of the applicability directive PSD II applies only to payment services provided within the European Union (EU). A shortcoming of this applicability directive is that where the service provider is not in connection with the territory of the EU the service TPP can be provided without any restrictions with the PSD II Directive, but also without the possibility of seeking by TPP from ASPSP particular behavior to which the entity is obliged by PSD II.[72]

The obligations imposed on ASPSP relating to access to payment accounts by TPP Concern only the case where these accounts are carried out by ASPSP online. The PSD II directive does not define what is meant by the availability of an online payment account. It is aptly assumed that this term should be understood broadly and encompasses cases of any form of communication of information systems of the parties in real time.[73]

Guarantee the ability to provide services to TPP, which are competitive and stand in opposition to the interests of the so-called. Payment service providers is art. 36 of the PSD II directive, which provides that each payment institution should have access to services provided under payment accounts. These services should be provided by ASPSP based on objective, non-discriminatory and proportionate rules. Any refusal to provide such services to TPP should be duly substantiated and notified to the supervisory authority – the Financial Supervision Commission.

TPP are not obligated to establish any contractual relationship with ASPSP. The requirement to cooperate ASPSP with TPP derives directly from directive PSD II.[74]

TPP in the case of provision of payment initiation services does not enter into any stage of payment transaction in the possession of cash. Where the TPP intends to do so shall be obliged to request the Financial Supervision Commission and obtain full authorization for the provision of payment services.

---

[70] Cf. K. Korus, *The notion of payment service in the payment services Act,* Monitor of Banking Law, July-August 2012, p. 33.

[71] Rightly K. Korus indicates that accounts linked to credits may be payment accounts. K. Korus, access-based services to the directive account PSD II, Monitor Banking Law, July-August 2017, p. 86; *Recommendation Council of banking Law and the Regulating the payment of the Union of Polish Banks on selected problems of interpretation of the Payment Services Act,* http://zbp.pl/public/repozytorium/dla_bankow/prawo/rada_prawa_bankowego/dzialalnosc/rekomendacja_grupa_robocza.doc [access: 25 X 2017*];* M. Mostowik, *Legal Protection of payment account information in the light of account information Services (AIS)*, Monitor of Banking Law, July – August 2017, p. 33.

[72] K. Korus, access-based services to the account in the PSD II directive, Monitor Banking Law, July-August 2017, p. 87.

[73] Ibid, pp. 87–88.

[74] Cf. Recital 30 to the preamble and Article 66 paragraph. 5 of the PSD II directive.

Payment Initiation Service (PIS) – general remarks

The PIS service is intended to expedite the performance of the contract by merchant (e.g. the shipment of goods through the online shop), because it gives him the guarantee of payment for goods or services-through PIS is initiated a specified electronic payment Merchant Payment Account as if you were doing it personally. Consent to the execution of a payment transaction granted by the payer through PIS is equivalent to the execution of a payment transaction expressed by the payer directly to the supplier.[75]

A model payment transaction scheme with the participation of PiS is such that the payment order of the payer (e.g. the person making the purchase in an online environment) is transferred to the ASPSP via the online banking provided to the user by ASPSP using the identification data agreed by the user of ASPSP, which is made available by the payer of PIS to initiate the payment transaction. The recipient of the cash is usually the seller of the goods, which is the contract with the PIS to handle such payments.[76] The PIS service allows you to make payments in an online environment without having to have a different payment instrument – e.g. Payment Card.[77]

Individual credentials used to secure user authentication (proof of identity by the provider), which the user or PIS use, are issued by the payment account provider (ASPSP).[78]

The PIS service was standardized in art. Article 4 (15) of the PSD II Directive and 66 of that directive. Essentially this service consists in placing the order by PIS on the command and on behalf of the user of a payment request to ASPSP to transfer funds to the account of the payee indicated by the user.[79] The main payment service which is the object of PIS is the transfer command.[80] The leading suppliers of these services are brands such as: Sofort[81] Whether Trustly.[82]

Payment Initiation Service (PIS) – regulatory issues

The Payment Initiation Payment service provider (PIS) may only be the payment service provider with such status according to the provisions of the Payment Services Act. In the case of a supplier having the status of a payment institution, it is necessary

[75] Article 64 paragraph. 2 of PSD Directive II.

[76] K. Korus, *Access-based services in the PSD II directive*, Monitor Banking Law, July-August 2017, p. 84.

[77] Recitals 28 and 29 to the preamble to the PSD Directive II.

[78] Recitals 30 to the preamble to the PSD Directive II.

[79] K. Korus, *Access-based services in the PSD II directive*, Monitor Banking Law, July-August 2017, p. 84.

[80] In the meaning of art. Article 3 (1) 4 UUP.

[81] https://www.sofort.com/pol-PL/kupujacy/sb/zakupy-online-z-sofort-banking/.

[82] https://trustly.com/pl/.

to extend the payment service authorization in respect of PIS and AIS.[83] Must have initial capital of 50 thousand euro.[84] The initial capital of such entities shall consist of one or more of the following elements:

- Equity instruments,
- Agio emissions related to capital instruments,
- Retained profits,
- Cumulated other total income,
- Reserve Capital.[85]

This is intended to constitute a guarantee element in case of adverse events related to the activity of TPP.

The payment service provider providing the PIS service should have a liability insurance or other comparable guarantee in order to be able to meet its obligations.[86] This regulation and the appropriate level of protection are of particular importance for the stability and security of the Bank (or other payment account holder), since in the event of an unauthorized payment transaction initiated by PIS, the ASPSP (e.g. the Bank) shall return without delay and in any event no later than the end of the following working day, the payer (customer) and the amount of the unauthorized transaction.[87] The subsequent order of the PIS, where he is responsible for the unauthorized transaction, shall compensate the ASPSP losses incurred or sums paid as a result of a refund to the payer, including the amount of the unauthorized payment transaction.[88]

Art. 66 PSD2 introduces the assumptions and regulatory framework of the PIS to the European legal order. The following are fundamental issues concerning the regulatory requirements imposed on the PIS and the ASPSP.

Duties of PIS:[89]

- The PSD II directive stipulates that the use of PIS is the right of the payer (the user) and ASPSP must respect this entitlement,
- PIS must obtain the payer's consent to initiate a payment order,
- The right to use the PIS is only available if the ASPSP leads to the user's online payment account,
- PIS does not at any time enter into possession of the payer's cash for the provision of the payment initiation service,

---

[83] Credit institutions within the meaning of Article 4 (1) 1, point 1 *Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms, amending Regulation (EU) No 648/2012* do not need dry authorization, in accordance with Article 11 (1) 1 of PSD Directive II.

[84] Article 7 point B PSD2

[85] Article 7 Directive II in ZW with Article 3. Article 26 (1) 1 point. A) to E) *Council Regulation (EU) no 575/2013 of 26 June 2013 on prudential requirements for credit institutions and investment firms, amending Regulation (EU) no. 648/2012.*

[86] Article 5 (1) 2 of PSD Directive II.

[87] Article 73 paragraph. 2 of PSD Directive II.

[88] Article 73 paragraph. 2 ph. 2 PSD Directive II.

[89] Article 66 paragraph. 1 and 3 of the PSD Directive II.

- PIS cannot change the amount of the payment order,
- PIS cannot change the payee of a payment order,
- PIS cannot alter any other features of the payment transaction,
- PIS must ensure that individual credentials of the user are not available to others (than the user and publisher of such data) of the parties,
- PIS must ensure that individual user credentials are transmitted through safe and efficient channels,
- PIS must ensure that all information about the payment service user is provided only to the payee and only to the expressly agreed payment service user,
- PIS is obliged each time a payment is initiated to identify itself to the payment service provider who holds the payer's payment account (ASPSP),
- The PIS is obliged to initiate payment, to communicate securely with the ASPSP, the payer and the consignee, in accordance with the provisions of article 5. 98 paragraph. 1 point. (d) PSD II directives[90],
- PIS may not store sensitive payment data,
- PIS may not require the payment service user of data other than the data necessary for the performance of the Payment initiation service,
- PIS may not use, obtain, or store any data for purposes other than for the provision of a payment initiation service expressly requested by the payer.

ASPSP obligations[91]:

- The ASPSP is obliged to communicate with the PIS in a secure manner, in accordance with the provisions of Article 98 paragraph. 1 point. (d) PSD II directives,
- ASPSP is obliged without delay after receiving a payment order from PiS to pass or make available all information about the initiation of the payment transaction and all information available to the ASPSP provider in relation to the execution of the transaction payment,
- The ASPSP must treat the payment orders transferred through the PIS, in a non-discriminatory manner, in relation to payment orders transferred directly ASPSP by the payer himself-in particular in terms of execution time, priority the nature of the levy, which, however, does not apply where

[90] EBA (European Banking Authority), in cooperation with the ECB (European Central Bank) and after consultation with all relevant stakeholders, including in the payment service market, develop draft regulatory technical standards RTS addressed to payment service providers specifying:

1. Requirements for strong client authentication,
2. Exclusions from the use of strong client authentication,
3. The requirements which security measures must fulfill to protect the confidentiality and integrity of the individual credentials of the payment service users,
4. Requirements for common and secure open standards of communication for the purpose of identifying, authentication, notification and information, as well as for the implementation of security measures, between ASPSP, the payer, the payee and the other payment service providers.

[91] Article 66 paragraph. 4 PSD Directive II.

discriminatory proceedings are justified by objective reasons,
– The performance of the PIS' services must not depend on the existence of a contractual relationship between the PiS and the ASPSP.

AIS – general remarks

The AIS service is regulated by Article 4 (16) and 67 of the PSD Directive II. This service consists of AIS access to the user's payment account (bank). Access to the account is based on the identifying data you have agreed with ASPSP. The user's data is provided by AIS. AIS logs in to the user's online banking system, and then collects and transmits aggregated data to the operator on-line communications. AIS thus obtains access to account data and for all payment transactions in that account.[92]

AIS – regulatory issues

Article 67 of the PSD Directive II introduces the AIS regulatory framework to the European legal order. The provision of AIS services does not require the authorization of the National Competent Authority (FSC), but only the registration.[93] The payment institution providing the AIS services should hold a liability insurance or other comparable guarantee in order to be able to meet its obligations.[94]
AIS responsibilities:
– The PSD II directive stipulates that the use of AIS is the payer's right (user) and ASPSP must respect this entitlement,
– AIS must obtain the user's consent to provide its services to him,
– The right to use the AIS services is granted to you only if the ASPSP leads you to a payment account available online,
– AIS must ensure that individual user credentials are not available to other parties, except for the user and the publisher of the user's personal authentication data,
– AIS must ensure that individual user credentials are transmitted by the AIS service provider through safe and efficient channels,
– AIS must identify themselves to ASPSP for each communication session,
– AIS must communicate with the ASPSP and the user in a safe manner and in accordance with the provisions of art. 98 paragraph. 1 point. (d) PSD II directives,
– AIS may only access information relating to payment accounts and related payment transactions,
– AIS may not request sensitive payment data relating to payment accounts,
– AIS may not use, obtain, store any data for purposes other than for the performance of the account information service explicitly requ-

[92] K. Korus, *Access-based services in the PSD II directive*, Monitor Banking Law, July-August 2017, p. 85, Article 67 paragraph 2 (a) (d) PSD Directive II.
[93] Article 33 and 5 (2). 3 PSD Directive II.
[94] Article 5 (1) 3 PSD PSD Directive II.

ested by the payment service user in accordance with the data protection regulations.

ASPSP obligations:

- ASPSP must communicate with AIS in a safe manner and in accordance with the provisions of Article 98 paragraph. 1 point. (d) PSD II directives,
- ASPSP must treat requests for data provided through AIS in a non-discriminatory manner, unless discriminatory treatment is justified by objective reasons,
- The supply of AIS services must not depend on the existence of a contractual relationship between AIS and ASPSP,
- As stated in the preamble of the PSD II directive, ASPSP provides all the information concerning the payment account, in particular the IBAN or NRB number, the amount of the balance, the transaction history (amount, title, date of execution, data of the other party[95]).

The leading suppliers of these services are: Kontomierz[96], AFAS[97], Tink[98], Money Dashboard[99], Quontis.[100]

CAF (Confirmation of the Availability of Funds) – General Comments

The PSD II directive introduces in addition to the aforementioned services TPP, also the process of confirming the availability of funds on the payer's payment account. However, this process is not a regulatory separate payment service.

This process enables the publisher of a payment instrument based on a credit card[101], previously designated ASPSP by the user (whose payment account provides the ASPSP) demand from ASPSP in real time, using online communication, information or on the user's account there is a certain amount. This process is therefore governed by the obligations of the ASPSP to the issuer of a payment instrument based on a credit card. It is your responsibility to inform ASPSP about your intention to use the CAF.[102]

---

[95] M. Mostowik, *Legal Protection of payment account information in the light of account information Services (AIS)*, Monitor of Banking Law, July – August 2017, p. 34.

[96] http://kontomierz.pl.

[97] https://www.afas.nl.

[98] https://www.tinkapp.com/en/.

[99] https://www.moneydashboard.com.

[100] http://www.qontis.ch.

[101] Instrument-based on payment card is a any payment instrument (among others card, mobile phone, computer) enabling initiation payment transaction they using the payment card system infrastructure – cf. Article 2, point 20 of the regulation of the European Parliament Council Regulation (EU) 2015/751 of 29 April 2015 on the fees interchange with respect to card-based payment transactions.

[102] K. Korus, *Access-based services in the PSD II directive*, Monitor Banking Law, July-August 2017, p. 85.

CAF – regulatory issues

It is ASPSP to confirm at the request of the supplier issuing payment instruments based on the card – availability on the payer's payment account the amount necessary for the execution of a card-based payment transaction.[103] (CAF service – Confirmation of the Availability Of Funds).

Legal requirements to applicability a CAF service:[104]

- the payment account of the payer must be accessible via the Internet at the time of the request for confirmation of availability of funds
- the payer has given ASPSP permission to respond to requests from a particular payment service provider to confirm that the amount corresponding to the specific payment transaction on the basis of the card is available on the payer's payment account,
- the consent for the ASPSP from the user to the story of the request must be given before the first request for confirmation.

Legal requirements imposed on the applicant supplier:

- the payer has granted this entity explicit permission to request the availability of cash,
- the payer has initiated a payment transaction executed using a card-based payment instrument,
- the CAF supplier must authenticate himself to the ASPSP provider,
- The CAF supplier must communicate with the ASPSP in a safe manner in accordance with the provisions of art. 98 paragraph. 1 point. (d) PSD II directives.

The confirmation of the availability of funds on a payment account by ASPSP is to answer "yes or no". Balance status is not fed. The CAF supplier may not store or use a response obtained from ASPSP for any purpose other than the execution of a card-based payment transaction.[105] Confirmation of availability of funds does not permit ASPSP to block a certain amount in the payer's account until the payment is settled.[106] For the implementation of the CAF service it is necessary to permit the issuance of card-based payment instruments.

Activities of TPP and cybersecurity

The prevention and countering of cybercrime in the area of payment infrastructure should be addressed, in addition to the eligible public entities, by industry financial organizations[107] (in cooperation with the relevant public services), as directly exposed

[103] Article 65 paragraph. PSD directive II.
[104] Ibidem.
[105] Article 65 paragraph. 3 PSD directive II.
[106] Article 65 paragraph. 4 PSD directive II.
[107] Cf. A. Marciniak, Bank CERT – New weapons in the fight against cybercrime [in:] A. Kawiński,

to threats and interested in the cybersecurity. An example of such an organization is FinansCERT from Norway.[108] This organization is CERT[109] in the Norwegian financial sector: banking and insurance. Its main tasks are:

- Tracing external threats,
- Support to combat attack and reduce losses,
- Coordination of cooperation with public institutions and order services (Interpol, police).

Other industry organizations whose activity is information security threats are among others established in the United States, but the global reach of non-governmental organizations: National Cyber-Forensics & Training Alliance (NCFTA), Financial Services Information Sharing and Analysis Center (FS-ISAC), SoltraWhether working in the European Union European Financial Institutes – Information Sharing and Analysis Centre (FI-ISAC).[110]

Bank Centre Cybersecurity

In September 2015, a recommendation on security and prevention of online banking inaccessibility was issued at the initiative of the Electronic Banking Council (PSV). The recommendation recommends that affiliated banks PSV established cooperation on:

- counteracting attacks on banks‘ e-banking platforms and their customers,
- responding to attacks.

The result of this recommendation was the establishment of the banking centre Cybersecurity BCC.[111] BCC is now one of the key platforms of the National Center Cybersecurity (NC Cyber).[112] BCC cooperates with the police and the National Clearing House S.A.,

A. Sieradz (ed.), *Challenges of Banking Informatics 2016*, Gdansk 2016, http://www.efcongress.com/sites/default/files/wyzwania_informatyki_bankowej_0.pdf, p. 187, [access: 2 X 2017].

[108] FinansCERT as an organization was established on 23 April 2013 in the Norwegian Industry organization umbrella Financial Institutions, http://www.finanscert.no [access: 15 X 2017].

[109] Computer Emergency Response Team – *Computer Incident Response Team.*

[110] A. Marciniak, Bank CERT– New weapons in the fight against cybercrime [in:] A. Kawiński, A. Sieradz (ed.), *Challenges of Banking Informatics 2016*, Gdansk 2016, http://www.efcongress.com/sites/default/files/wyzwania_informatyki_bankowej_0.pdf, p. 187, [access: 25 X 2017]

[111] See the BCC open information on the PSV website. https://zbp.pl/wydarzenia/archiwum/wydarzenia/2016/lipiec/otwarcie-bankowego-centrum-cyberbezpieczenstwa [access: 25 X 2017]; Until Streżyńska, reply to interpellation, BM-WOP. 072.69.2017, Warsaw 22.06.2017, http://www.sejm.gov.pl/Sejm8.nsf/InterpelacjaTresc.xsp?key=75AD31FB, [access 25 X 2017], A. Marciniak, Bank CERT – New weapons in the fight against cybercrime [in:] A. Kawiński, A. Sieradz (ed.), *Challenges of Banking Informatics 2016*, Gdansk 2016, http://www.efcongress.com/sites/default/files/wyzwania_informatyki_bankowej_0.pdf, p. 191, [access: 25 X 2017]. 191 [access: 3 X 2017].

[112] NCC was established on 4 July 2016 and operated in the NASK structure (scientific and academic computer network), which is a state research institute within the meaning *Act of 30 April 2010 on research Institutes*. According to paragraph 3 (a) of 2 (1 Point D *of the Council of Ministers of 7 June 2017 on the giving of the scientific and academic network of the statutes of Status of State Research Institute* (Journal of laws 2017, item 1193). DNASK tasks should be to ensure cybersecurity public entities through the development of the National Cybersecurity.

telecommunications operators, quick payment operators, exchanges bitcoin.[113] In the event of a risk to cybersecurity BCC becomes the crisis staff, which manages the crisis situation in the banking sector. Currently, the focus of BCC is in particular:

- Monitoring of the banking sector in terms of Cybersecurity and to respond to hazards,
- Communication management in particular by:
  a) Developing a coherent information policy for customers and media in the banking sector, the main objective of which is to inform immediately of any risks Cybersecurity or failure of electronic banking systems,
  b) Develop communication procedures between participants,
  c) The elaboration of cooperation and communication channels with law enforcement agencies, other CERT, software producers and security systems,
- Defining and monitoring the implementation of preventive measures in the sector.[114]

We can easily imagine situations in which TPP in the initial phase of the activity, building its reputation in the market and user confidence, after a while having already had the data to log into the accounts of the clients ' bank, leads to mass to a number of unauthorized transactions. These transactions against clients allegedly using the PIS service are, in the first instance, legally and financially responsible for the bank. The Bank has a claim to TPP for reimbursement of amounts that are the subject of unauthorized transactions, which can however be satisfied only if the TPP is solvent. Another example is possible when AIS has a database of sensitive credentials to log in to bank accounts and intentionally leads to loss of such a database. Costs, not only financial (due to very large volume and volume of payment transactions), but social (caused by loss of customer confidence in the payment ecosystem) can be difficult to quantify. Even if the caused damage is covered in full, the significant resulting cost will be the loss of confidence in the financial sector by customers.

Taking the above into account, the activities of TPP can also cause significant legal problems on the plane:

- Banking secrecy[115],
- Payment secrecy[116],
- Rights to the protection of personal data,
- Rights of privacy, such as the holder of the account and third parties whose personal data appear in the electronic banking application, as paying or recipients.[117]

---

[113] A. Marciniak, Bank CERT – New weapons in the fight against cybercrime [in:] A. Kawiński, A. Sieradz (ed.), *Challenges of banking Informatics 2016*, Gdansk 2016, http://www.efcongress.com/sites/default/files/wyzwania_informatyki_bankowej_0.pdf, p. 193, [access: 25 X 2017].

[114] Ibid., p. 193.

[115] See. Article 104 paragrapf 1 *Act of 29 August 1997 Banking Law* (OJ no 140, item 939, Subsequent. D.).

[116] See. Article 11 (3) 1 UUP.

[117] To the extent indicated risks Cf. M. Mostowik, *Legal Protection of payment account information*

Summary

The services of TPP are currently and will continue to be present in the electronic payments segment, and their even greater growth will occur when they are permanently aggregated with providers of social networks and mass services such as: Facebook, Apple, Amazon, NetflixGoogle[118], Uber Spotify.

Both the payment initiation service providers (PIS) and the payment account service provider (AIS) on one side and the traditional payment service providers on the other should respect the data protection requirements and PSD II and the RTS directive. The RTS should ensure the interoperability of[119] different communication solutions from a technological point of view. The RTS should also allow the payment account provider (ASPSP) to know that the payment transaction is in contact with the PIS and not the client directly.[120]

It should be noted that the provisions of the PSD II directive on the activities of TPP are very general. All the important technical issues to ensure the security of these services and the entities using them and providing them have been settled by the RTS. In view of the fact that the services of TPP are provided inter alia in an Internet environment, malfunctions in their operation may pose a threat to cybersecurity of the paying critical infrastructure. The Association of Polish Banks constantly monitors the factual and legal situation, noting the risks associated with the activity of TPP.[121]

The legal architecture contained in the PSD II directive in the field of TPP, is an example of effective regulatory lobbying of entities providing these services for years. Players who are TPP, due to potential risks at the micro-scale (loss of funds by the user) and macro (threat to the payment operation of critical infrastructure) should meet with the prudential approach of the regulator – Supervisory Committee and users in the early stages of operation.

Abstract

Online and mobile payments due to their non-cash character and speed are characterized by very high development potential. As their volume and quota increase, the risks associated with their processing are increasing, as they do not involve the physical participation of the parties and the Internet environment. New payment methods

in the light of account information Services (AIS), Monitor of Banking Law, July – August 2017, pp. 35–42.

[118] Specified in short FAANG (Facebook, Apple, Amazon, NetflixGoogle).

[119] A feature of the product or system whose interfaces enable it to work with other products or systems.

[120] Recital 93 to the preamble to Directive PSD II.

[121] Based on note Restrictions Services based on third party access (PISP, AISP) to payment accounts in the light of the PSD2 of the Banking Council of the Polish Bank Association, https://zbp.pl/public/repozytorium/wydarzenia/images/luty_2017/Polish_Bank_Association_Notatka_PL_Third_Party_Services_PSD2_January_2017_fin.pdf [access: 10 X 2017].

have led to the emergence of new suppliers – the so-called Third Party Payment Service providers-payment service providers which are third parties whose activities may involve specific threats. At the micro scale, you can indicate the security risks of your financial resources. On a macro scale, you should indicate the potential risks to the so-called of paying critical infrastructure and more broadly - cybersecurity.

Keywords: PSD, cybercrime, Third Party Providers, critical infrastructure, Financial Supervision Commission, electronic payment transactions, mobile payments, online payments, Account Servicing Payment Service Provider, Account Information Service, Payment Initiation Service.