ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA PRÁVNICKÁ

Katedra finančního práva a národního hospodářství

DIPLOMOVÁ PRÁCE

Vybrané otázky zákona o platebním styku v souvztažnosti se směrnicí PSD2

Huy Ho Ba

Plzeň, 2021

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta právnická
Akademický rok: 2020/2021

ZADÁNÍ DIPLOMOVÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Huy HO BA**
Osobní číslo:	**R16M0078P**
Studijní program:	**M6805 Právo a právní věda**
Studijní obor:	**Právo**
Téma práce:	**Vybrané otázky zákona o platebním styku v souvztažnosti se směrnicí PSD2**
Zadávající katedra:	**Katedra finančního práva a národního hospodářství**

Zásady pro vypracování

1. Úvod
2. Obecně o novinkách ZPS v návaznosti na směrnici PSD2
3. Silné ověření klienta při poskytnutí platební služby
4. Vybrané novinky ovlivňující FinTech
5. Závěr

Rozsah diplomové práce:
Rozsah grafických prací:
Forma zpracování diplomové práce: **tištěná**

Seznam doporučené literatury:

- Zákon č. 370/2017 Sb., o platebním styku
- Důvodová zpráva k zákonu č. 370/2017 Sb., o platebním styku
- Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu
- PSD2: malá revoluce v platebních službách. Hospodářské noviny [online]. [cit. 2020-06-15]. Dostupné z: https://ictrevue.ihned.cz/c3-65786220-0ICT00_d-65786220-psd2-mala-revoluce-v-platebnich-sluzbach
- Nový zákon o platebním styku a největší změny, které přináší. *Epravo.cz* [online]. Dostupné z: https://www.epravo.cz/top/clanky/novy-zakon-o-platebnim-styku-a-nejvetsi-zmeny-ktere-prinasi-106626.html
- PSD2 a GDPR: Harmonie, či disonance? *Právní rádce* [online]. Dostupné z: https://pravniradce.ihned.cz/c1-65909940-psd2-a-gdpr-harmonie-ci-disonance
- Co přináší nový zákon o platebním styku? *Právní rádce* [online]. Dostupné z: https://pravniradce.ihned.cz/c1-66010790-co-prinasi-novy-zakon-o-platebnim-styku
- *FinTech v ČR i ve světě – Vliv nových technologií na finanční sektor* [online]. In: . Dostupné z: https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/FinTech_v_CR_i_ve_svete_v2.pdf

Vedoucí diplomové práce: **JUDr. et Mgr. Silvie Anderlová**
Katedra finančního práva a národního hospodářství

Datum zadání diplomové práce: **12. března 2020**
Termín odevzdání diplomové práce: **31. března 2021**

Západočeská univerzita v Plzni
Fakulta právnická
L.S.

JUDr. et PhDr. Stanislav Balík, Ph.D.
děkan

JUDr. Petra Hrubá Smržová, Ph.D.
vedoucí katedry

V Plzni dne 27. července 2020

Prohlášení

„*Prohlašuji, že jsem tuto diplomovou práci zpracoval samostatně, a že jsem vyznačil prameny, z nichž jsem pro svou práci čerpal způsobem ve vědecké práci obvyklým.*“

Plzeň, březen 2021

_____

Huy Ho Ba

Poděkování

Tímto bych chtěl poděkovat vedoucí diplomové práce, paní JUDr. et Mgr. Silvii Anderlové za rady a připomínky během zpracování této práce. Touto cestou bych chtěl rovněž poděkovat rodičům za neutuchající podporu během celého studia.

Obsah

Seznam použitých zkratek

Směrnice PSD	Směrnice Evropského parlamentu a Rady 2007/64/ES ze dne 13. listopadu 2007 o platebních službách na vnitřním trhu
Směrnice PSD2	Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu
Nařízení RTS	Nařízení Komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace
ZoPS	zákon č. 370/2017 Sb., o platebním styku
ZoPS z 2009	zákon č. 284/2009 Sb., o platebním styku

Úvod

Byť si to možná neuvědomujeme, ale s úpravami zákona o platebním styku se setkáváme každý den. Během nákupů v supermarketu, při převodu peněz z jednoho účtu na druhý nebo nočních nákupů na e-shopu, když člověk trpí nespavostí. Téma nového zákona o platebním styku bylo s příchodem účinnosti v lednu 2018 hojně diskutováno, avšak si nemyslím, že bylo tomuto tématu učiněno za dost.

Měl jsem tu čest během studia získávat zkušenosti v advokátních kancelářích, jmenovitě Clifford Chance, Havel & Partners a Deloitte Legal, které mě ve velkém ovlivnily, jak lidsky, tak zejména ve vnímání práva a neoddělitelné vazbě ke společnosti a jeho regulaci. Zejména v Havel & Partners jsem se poprvé dostal k opravdové právní práci, a i díky příležitostem z regulatorní části na oddělení Banking & Finance, mě zaujala tématika zákona o platebním styku, ke kterému jsem dělal nespočet rešerší v době, kdy zákon o platebním styku byl vcelku novou úpravou a neexistoval k němu komentář a odborná veřejnost začala utvářet názor.

Zejména v době, kdy jsem si měl vybrat téma na svou diplomovou práci, se v médiích objevily zprávy typu „velká, zlá“ Evropská unie opět České republice něco diktuje. Tentokrát šlo o to, že možná nebudeme moci platit kartou bezkontaktně do částky 500 Kč a budeme muset při každém placení potvrzovat PINem jako při kontaktní platbě. I proto jsem se rozhodl, že chci prozkoumat novinky, které přináší směrnice PSD2 z roku 2015, a kterou český zákonodárce implementoval do nového zákona o platebním styku.

Vzhledem k tomu, že mě vždy lákal IT obor a nové technologické vychytávky, chci se v této diplomové práci zaměřit zejména na oblast, která se dotýká FinTech a zjistit, zda zákonodárce byl tentokrát o krok před v zavedení nových regulací k novým službám či pouze ex-post dotváří zákonný rámec službám, které jsou už na trhu zavedené, ale nebyly legislativně upraveny.

Cílem této diplomové práce je představit vybrané novinky ze zákona o platebním styku, ve spojení se směrnicí PSD2. Budu se zabývat, jak jsou zavedené tyto novinky do praxe a zda jsou mezi uživateli používány nebo jsou tyto služby nevyužité.

Má diplomová práce je členěna do čtyř kapitol. V první kapitole se budu věnovat obecně o směrnici PSD2, kde se budu zaobírat novinkami, které se

implementovaly do ZoPS a porovnávat nejviditelnější změny s minulou úpravou ZoPS z 2009, nýbrž se směrnicí PSD.

V druhé kapitole se budu zabývat FinTechem a využití novinek v návaznosti na směrnici PSD2. V této kapitole se budu zabývat zejména novými službami nepřímé dání platebního styku a informováním o platebním účtu, jak jsou upraveny v ZoPS a jak jsou v praxi využity bankami, třetími stranami a uživateli. Neopomenu však ani fenomén open bankingu, jeho různé standardy v členských zemích nebo některé asociace, které v České republice udávají trendy ve FinTech. V neposlední řadě se budu zabývat aplikacemi, které využívají nové služby zavedení směrnicí PSD2.

Třetí kapitola bude věnována silnému ověření uživatele, které s příchodem směrnice PSD2 bylo jedním z regulatorních požadavků, které pocítili uživatelé na vlastní kůži a bylo pro mě prvotním impulzem k napsání této diplomové práce. Budu se zabývat tím, jak je legislativně upraven v ZoPS, jaké jsou jednotlivé prvky ověření a v jakých případech se užije silné ověření uživatele. Neopomenu ani výjimky z nařízení RTS, při které se nemusí provádět silné ověření uživatele.

V poslední kapitole rozeberu snížení limitu odpovědnosti plátce při neautorizované platební transakci, která se snížila ze 150 EUR na 50 EUR. Zejména s ohledem na podmínky, které vylučují spoluúčast plátce při neautorizované platební transakci nebo na ty případy, kdy plátce bude muset nést plnou odpovědnost.

1. Obecně o směrnici PSD2, ZoPS a komparace s předešlou právní úpravou

Směrnice PSD2 byla přijata 25. listopadu 2015, která plně nahradila směrnici PSD2 a měla být následně implementována do vnitrostátních právních řádů členských států. Česká republika jej implementovala pomocí ZoPS, který je platná od 11. října 2017 a účinná od 13. ledna 2018, které bylo datumem, kdy měla být směrnice PSD2 provedena napříč členskými státy Evropské unie.

Nedalo by se říct, že ZoPS měl za sebou jednoduchý legislativní proces[1], jelikož návrh byl předložen vládou už v březnu 2017, avšak byla schválen až v říjnu 2017, těsně před lhůtou, kdy měla Česká republika mít implementovanou směrnici PSD2 ve svém právním řádu.

Směrnice PSD, která byla přijata 13. listopadu 2007 měla za cíl „zavést jednotný systém pravidel pro poskytování platebních služeb v Evropské unii a Evropském hospodářském prostoru (EHP) a zajistit, aby platby do zahraničí byly jednodušší a pružnější“[2], díky čemuž se zrodila „komplexní regulatorní rámec poskytování platebních služeb“[3]. I když by se dalo nabýt pocitu, že tento regulatorní rámec byl dostačující, tak zdaleka nebyl. Různé mezery, obecnosti, kterými směrnice PSD trpěla, vytvořily problémy v podobě regulatorních arbitráží[4], rozdílné poplatky za platební služby[5] nebo „standardizace řešení a zabezpečení byla ze strany operátorů za svou nedostatečnost rovněž kritizována“[6]. Díky směrnici PSD nebankovní společnosti mohly provádět finanční transakce[7], banky a poskytovatelé museli „být transparentní ve svých službách a poplatcích, musí například uvádět nejzazší časy provedení platby, poplatky a směnné kurzy“[8].

---

[1] VOJTĚCH, Petr. Nový zákon o platebním styku v platnosti. *Epravo.cz* [online]. 2017 [cit. 2021-03-16]. Dostupné z: https://www.epravo.cz/top/clanky/novy-zakon-o-platebnim-styku-v-platnosti-106689.html?mail

[2] Novela poskytování služeb. Euro.cz [online]. [cit. 2021-03-16]. Dostupné z: https://www.euro.cz/archiv/novela-poskytovani-sluzeb-823214

[3] VOJTĚCH, Petr. Nový zákon o platebním styku v platnosti. *Epravo.cz* [online]. 2017 [cit. 2021-03-16]. Dostupné z: https://www.epravo.cz/top/clanky/novy-zakon-o-platebnim-styku-v-platnosti-106689.html?mail

[4] Ibid.

[5] KŘÍŽ, Lukáš a David ZAJÍC. PSD2: malá revoluce v platebních službách. *Hospodářské noviny* [online]. [cit. 2021-03-16]. Dostupné z: https://ictrevue.ihned.cz/c3-65786220-0ICT00_d-65786220-psd2-mala-revoluce-v-platebnich-sluzbach

[6] Ibid.

[7] Co PSD1 a PSD2 znamenají a proč jsou důležité? *IBanFirst Blog* [online]. 2018 [cit. 2021-03-16]. Dostupné z: https://blog.ibanfirst.com/cz/co-psd1-a-psd2-znamenaj%C3%AD-a-pro%C4%8D-jsou-d%C5%AFle%C5%BEit%C3%A9

[8] Ibid.

Odborná veřejnost a adresáti směrnice PSD oprávněně čekali zlepšení tohoto stavu, což směrnice PSD2 se snažila předchozí chyby ze směrnice PSD napravit. Kromě náprav se zaměřila směrnice na nové služby, které byly legislativně podchyceny. Jmenovitě například služba informování o platebním účtu (viz kapitola 2.4.) a služba nepřímé dání platebního příkazu (viz kapitola 2.5.). Snažila zvýšit bezpečnost internetových plateb, a to pomocí silného ověření uživatele (viz kapitola 3.).

Novými službami informování o platebním účtu a službou nepřímého dání platebního příkazu směrnice PSD2 donutila banky k tomu, aby otevřely data svých uživatelů třetím stranám, díky čemuž může profitovat jak FinTech společnosti, tak i uživatelé, kteří díky tomu získají nové služby (viz kapitola 2. a dále).

ZoPS oproti ZoPS 2009 rozšiřuje subjekty, které jsou oprávněny poskytovat platební služby, a to o držitele poštovní licence, jehož poštovní licence výslovně obsahuje službu dodání peněžní částky poštovním poukazem.[9] Držitelé poštovní licence „doposud umožňoval těmto subjektům pouze provádět převod peněžních prostředků prostřednictvím poštovního poukazu, který není služnou platební, ale službou poštovní.“[10] Nesmím opomenout ani správce informací o platebním účtu (viz kapitola 2.4.2. a dále).

Změna, která se dotkne všech plátců, je snížení limitu odpovědnosti při neautorizované platební transakci (viz kapitola 4.) z částky 150 EUR na 50 EUR. Neautorizovaná platební transakce nastává nejčastěji například při odcizení nebo ztrátě platební karty.

[9] § 5, písm. l) zákona č. 370/2017 Sb., o platebním styku

[10] VOJTĚCH, Petr. Nový zákon o platebním styku v platnosti. Epravo.cz [online]. 2017 [cit. 2021-03-16]. Dostupné z: https://www.epravo.cz/top/clanky/novy-zakon-o-platebnim-styku-v-platnosti-106689.html?mail

2. FinTech a využití novinek v návaznosti se směrnicí PSD2

V dnešní době se skloňuje slovo FinTech čím dál více ve světě financí a rovněž se často vyskytuje ve slovníku osob pohybující se v oboru bankovního práva.

Pojem FinTech je složeninou slov finance a technologie. Jde o nové technologie, které se uplatňují ve finančním sektoru, zároveň jde i o společnosti a finanční platformy, které inovují poskytování finančních služeb. Obecně do FinTech spadají inovativní a nové produkty finančního sektoru, které narušují pořádky v tomto sektoru.[11]

Souhrnně pojem FinTech pojme například „mobilní platby, kryptoměny, crowdfunding nebo on-line platformy na poskytování mikropůjček“.[12] „Konkrétně se pak z hlediska podnikatelského vztahuje ke společnostem, které využívají sociální sítě, rozšířenou inteligenci (včetně samoučících se programů), mobilní aplikace, distribuované databáze (DLT), jako je především blockchain, datacloudy nebo jiný software, zkrátka moderní technologie k tomu, aby poskytování bankovních, investičních nebo jiných finančních služeb bylo efektivnější. Jedná se buď o samotné poskytovatele těchto služeb (například poskytovatele spotřebitelských úvěrů, platebních či investičních služeb), nebo osoby, které těmto poskytovatelům pomáhají lépe zacílit na zákazníky či rozvíjet jejich podnikání (IT společnosti vyvíjející API, crowdfundingové platformy, účetní cloudy aj.)“.[13]

Právně nebyly FinTech přímo regulovány českou legislativou, nýbrž zejména evropskou legislativou (pokud nezahrnuji crowdfunding)[14]. Směrnice PSD2 se dá pokládat jako jednou z vlaštovek této regulace, pokud nebudeme počítat anti-money laundering (AML) směrnice.

Nejen v právním světě, ale i ve finančním světě se čím dál více rozrůstá disrupce starých pořádků a s příchodem nových technologií, jako jsou chytré telefony, využívají finanční start-upy, technologické společnosti, a i banky příležitosti, jak získat zákazníka z pohodlí domova, přes internet.

---

[11] FinTech v ČR i ve světě. In: *Deloitte Česká republika* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/FinTech_v_CR_i_ve_svete_v2.pdf, s. 4

[12] ŠOVAR, Jan a Ondřej MIKULA. FinTech v Česku: Legislativní iniciativa míří výlučně z Bruselu. *Právní rádce* [online]. 2017 [cit. 2021-02-22]. Dostupné z: https://pravniradce.ihned.cz/c1-65872700-fintech-v-cesku-legislativni-iniciativa-miri-vylucne-z-bruselu

[13] Ibid.

[14] Ibid.

Z hlediska bank to znamená v budoucnu úspory za provoz poboček (při plánovaném postupném zavírání), lidského kapitálu (propouštění pracovníků na pobočkách), ale hlavně snaha neustrnout ve vývoji a přizpůsobovat se současným trendům, které udávají zejména start-upy. V posledních měsících můžeme v médiích sledovat zprávy o hromadných propuštěních, jako například v Komerční bance, Česká spořitelně nebo ČSOB, které budou redukovat počet poboček a zaměstnanců.[15]

Pro klienta to může být přínosné zejména lepší dostupností finančních služeb, spočívající v jejich přístupnosti v kteroukoliv denní dobu a na kterémkoliv místě, zejména pokud bydlí mimo dosah fyzických poboček bank, například v malé vesnici.

Ruku v ruce jsou tu ale také nevýhody a rizika plynoucí z tohoto způsobu fungování. Hrozí větší kybernetické riziko, odcizení citlivých údajů klientů[16] a nedůvěra konzervativních klientů banky, kteří upřednostňují osobní kontakt s bankéřem na pobočce. V každém případě model uzavírání všech poboček bank není stále na pořadu dne[17], ale pandemie koronaviru COVID-19 uspíšila přechod klientů k bankovním aplikacím dostupných na chytrých telefonech či k internetovému bankovnictví.

Pro start-upy to znamená obrovskou příležitost dostat část podílu na trhu od bank, které velké portfolio produktů, které mohou kombinovat při nabídce pro své klienty. Start-upy se zaměřují na určité produkty nebo přímo sektory a směrnice PSD2 jim dává příležitost získat klientelu právě od bank, pomocí otevřeného API (Application Programming Interface). Pro banky nejsou tyto start-upy zatím přímo soupeři, jelikož se start-upy stále zabývají určitými produkty a některé banky dokonce přímo spolupracují se start-upy. Například Komerční banka, která navázala spolupráci s BudgetBakers.[18]

---

[15] ZATLOUKAL, Jiří. Pokračuje propouštění v bankách. Komerčka se zbaví čtvrtiny zaměstnanců. *Seznam Zprávy* [online]. 2021 [cit. 2021-02-22]. Dostupné z: https://www.seznamzpravy.cz/clanek/pokracuje-propousteni-v-bankach-komercka-se-zbavi-ctvrtiny-zamestnancu-142061

[16] FinTech v ČR i ve světě. In: *Deloitte Česká republika* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/FinTech_v_CR_i_ve_svete_v2.pdf, s. 11

[17] BUŘÍNSKÁ, Barbora. Klienti se přesouvají do onlinu, velké banky zavírají pobočky. *Novinky.cz* [online]. 2020 [cit. 2021-02-22]. Dostupné z: https://www.novinky.cz/finance/clanek/klienti-se-presouvaji-do-onlinu-velke-banky-zaviraji-pobocky-40340316

[18] Komerční banka spolupracuje s BudgetBakers. In: *Komerční banka* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://www.kb.cz/cs/o-bance/pro-media/tiskove-zpravy-2019/komercni-banka-spolupracuje-s-budgetbakers

Dále jako příklad může sloužit český start-up Spendee, který se zabývá správou financí. Díky otevřenému API nemusí jejich uživatel zadávat manuálně všechny platby, které provedl za daný den, ale Spendee si sám stáhne informace od banky přes službu informování o platebním účtu (viz kapitola 2.4.), která je nově zavedena díky směrnici PSD2 do ZoPS. S takovými možnostmi získává klient do rukou mocné nástroje, které může například využít k lepší finanční správě, ve zmiňovaném Spendee nebo třeba BudgetBakers.

S nástupem směrnice PSD2 se očekávalo, že v České republice bude více FinTechů, které využijí mezery na trhu, avšak opak je pravdou.[19] Jednou z příčin může být zejména zdlouhavý a náročný průběh a zejména podmínky nutné k získání povolení k činnosti od České národní banky (viz kapitola 2.2.3.).[20]

Výše zmiňované služby nepřímého dání platby a služba informování o platebním účtu jsou uvedeny v ustanovení § 3, odst. 1 ZoPS, v písmenu g), respektive h), které jsou mezi platebními službami. To znamená, že se vztahuje na poskytovatele služby nepřímého dání platby a služby informování platebního účtu kritéria platební instituce, která je oprávněna poskytovat platební služby na základě povolení k činnosti platební instituce.[21] [22] V povolení k činnosti platební instituce Česká národní banka uvádí platební služby, na které se povolení vztahuje.[23] To znamená, že platební instituce může požádat o určitý okruh platebních služeb, které bude poskytovat a nemusí zahrnout v sobě všechny možnosti, které ZoPS v ustanovení § 3 udává. Zvláštností je to, že například žádost o povolení k činnosti pro správce informování o platebním účtu se podává pouze elektronicky[24].

Vyhláška č. 1/2018 Sb., o žádostech a oznámeních k výkonu činnosti podle zákona o platebním styku a vyhláška č. 7/2018 Sb., o některých podmínkách výkonu činnosti platební instituce, správce informací o platebním účtu, poskytovatele platebních služeb malého rozsahu, instituce elektronických peněz

[19] HINGAR, Petr. Otevřené bankovnictví, PSD2, open API a BankID aneb Změna paradigmatu ve finančním sektoru. *SystemOnline.cz* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://www.systemonline.cz/it-pro-banky-a-financni-organizace/otevrene-bankovnictvi-psd2-open-api-a-bankid.htm

[20] VEJVODOVÁ, Alžběta. Platební revoluce se nekoná. O licence na nové služby není v Česku zájem. *Právní rádce* [online]. 2018 [cit. 2021-02-22]. Dostupné z: https://pravniradce.ihned.cz/c1-66152590-platebni-revoluce-se-nekona-o-licence-na-nove-sluzby-neni-v-cesku-zajem

[21] § 7 zákona č. 370/2017 Sb., o platebním styku

[22] § 8 Ibid.

[23] § 10 Ibid.

[24] § 10, odst. 1 Ibid.

a vydavatele elektronických peněz malého rozsahu upravují náležitosti těchto žádostí a podmínky k výkonu činnosti.

Výše se zmiňuji o zdlouhavosti udělení povolení k činnosti, ZoPS udává lhůtu 3 měsíce[25] od zahájení řízení, který je správním řízením[26]. To by se mohlo zdát, že je dost krátká doba, avšak pokud žádost nemá předepsané náležitosti či trpí jinými podstatnými vadami, zastavuje se běh lhůty a obnoví se až po odstranění těchto vad. Často toto řízení zdržuje nedokonalý obchodní plán a nepřizpůsobené vnitřní předpisy těchto právnických osob, které se uchází o licenci[27]. Ve výsledku tyto chyby zapříčinily, že některé české společnosti, jmenovitě například Spendee, nestihly nástup konkurence z ostatních zemí v Evropské unii a jsou na tom teď biti.

Samotné požadavky z výše uvedených vyhlášek je dle mého názoru složité splnit a vyžaduje obrovské množství času, úsilí, a hlavně finančních prostředků k zhotovení podání samotné žádosti. Nepočítám ani vynaložení určité části rozpočtu budoucího poskytovatele platebních služeb pro právní zastoupení, jelikož si myslím, že právní laik nemá šanci je splnit a být v souladu se všemi právními předpisy.

2.1. Česká fintech asociace

České fintech společnosti mají vlastní asociaci, ve které se sdružují. Česká fintech asociace vznikla v září 2016. Účelem této asociace je „poskytování obecně prospěšných služeb především v oblasti vedení a propagace odborné diskuse v oblasti rozvoje poskytování finančních služeb za pomoci internetu a moderních informačních a telekomunikačních technologií (dále jen FinTech) mezi zástupci uživatelů, právnických a fyzických osob, organizací akademické, veřejné a neziskové sféry, dále vzdělávání veřejnosti ohledně nových možností a příležitostí, které poskytuje FinTech, a celková podpora odvětví FinTech“[28]. Uvnitř asociace jsou založeny pracovní skupiny pro legislativu a krypto assets.[29] Pořádají vzdělávací semináře, konference a vydávají analýzy.

---

[25] § 10, odst. 2 zákona č. 370/2017 Sb., o platebním styku

[26] BERAN, Jiří. § 10 [Řízení o žádosti o udělení povolení k činnosti platební instituce]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[27] TÓTHOVÁ, Lucia. Jak těžké je získat PSD2 licenci? *#fintechcowboys.cz* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://fintechcowboys.cz/rozhovor-jak-tezke-je-ziskat-psd2-licenci/

[28] Výpis ze spolkového rejstříku - Česká fintech asociace, z.s., L 66392 vedená u Městského soudu v Praze. *Veřejný rejstřík a sbírka listin* [online]. [cit. 2021-03-15]. Dostupné z: https://or.justice.cz/ias/ui/rejstrik-firma.vysledky?subjektId=944463&typ=PLATNY

[29] Projekty a znalosti. *Česká fintech asociace* [online]. [cit. 2021-03-15]. Dostupné z: http://czechfintech.cz/projekty-a-znalosti/

Jejich řádní členové jsou aktivní v oblasti FinTech[30]. Mezi řádné členy patří výše zmínění BudgetBakers a Spendee. Nelze však opomenout další známé společnosti, jako jsou GoPay, MallPay nebo Twisto.

2.2. Česká bankovní asociace

Banky v České republice mají taktéž svou vlastní asociaci, ve které se sdružují. Česká bankovní asociace vznikla v únoru 1992 a má za cíl „rozvoj českého bankovního sektoru, celé naší ekonomiky a finanční gramotnosti Čechů."[31] Asociace pořádá konference, provozuje vzdělávací projekty jako například Bankéři do škol, #BezpecneBanky[32]. Je součástí Evropské bankovní federace, Evropské rady pro platby, Evropského ústavu pro peněžní trhy. Angažuje se v prevenci kriminality, udržitelnosti a zejména ve snížení uhlíkové stopy během poskytování služeb.[33] Sdružuje 37 bank, což představuje 99 % bankovního trhu.[34] Není třeba více představovat například Českou spořitelnu, Komerční banku a další velké banky.

Česká bankovní asociace je průkopníkem v digitalizaci, což dokazuje projektem Českého standardu pro Open banking (níže v kapitole 2.3.1.) a nově průlomovou tzv. bankovní identitu, která byla schválena loni pod zákonem č. 49/2020 Sb. Tento zákon je nominovaným v anketě Zákon roku 2020 pořádaná advokátní kanceláří Deloitte Legal.

2.3. Open banking standard

Už před příchodem směrnice PSD2 se hodně mluvilo o open banking trendu, který otevírá přístup k datům klientům bank pro třetí strany. Směrnice PSD2 určuje, které služby mají být dostupné pro třetí stranu, jmenovitě služba nepřímé dání platebního příkazu, služba informování o platebním účtu a služba potvrzování zůstatku peněžních prostředků pro vydavatele karetních prostředků (zkráceně CIS), však nevytvořila jednotný standard, který by vyřešil přístup třetích stran k datům o klientech, a proto různé asociace, skupiny vytvořily svůj vlastní open banking

[30] Stanovy České fintech asociace, z.s., *Česká fintech asociace* [online]. [cit. 2021-03-15]. Dostupné z: http://czechfintech.cz/wp-content/uploads/2018/01/Stanovy_Ceska_fintech_asociace.pdf

[31] Kdo jsme a co děláme. *Česká bankovní asociace* [online]. [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/co-delame

[32] Naše projekty. *Česká bankovní asociace* [online]. [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/nase-projekty

[33] Kdo jsme a co děláme. *Česká bankovní asociace* [online]. [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/co-delame

[34] Členové asociace. *Česká bankovní asociace* [online]. [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/clenove

standard, jako například v České republice nebo ve Velké Británii.[35] Tyto standardy by měly poskytnout základní technický rámec pro API bank, které se zúčastní daného standardu.[36] Rozdíl v těchto standardech můžeme najít například v tom, že mají: „Jiné sady URL, jiné HTTP metody u semanticky stejných API, jiné struktury JSON request/response objektů.“[37] Což jsou zkrátka technické specifikace pro API, které Evropská unie ve směrnici PSD2 neupravila.

API je zkratkou pro Application Programming Interface, „rozumí se tím rozhraní pro aplikace a jejich programování. Jedná se o balík knihoven, funkcí, procedur, protokolů a tříd, které mohou programátoři používat pro komunikaci se softwarem. Funkce rozhraní jsou na bázi programových celků, které programátoři používají a nemusejí je tak sami programovat. Cílem API je komunikace mezi 2 aplikacemi, kterým je tak umožněna výměna dat. Komunikaci lze nastavit jak jednosměrnou, tak i obousměrnou.“[38]

Přístup přes API je dle mého názoru klíčovým pro FinTech sektor, zejména pro poskytovatele služby informací o platebním účtu a poskytovatele služby přímé dání platebního příkazu, jelikož není třeba vyžadovat od uživatele těchto služeb jeho přístupové údaje do jeho internetového bankovnictví a přístup přes screen scraping, který je těžkopádný a každá malá změna v internetovém bankovnictví může znehodnotit získaná data. Open banking by měl tuto zastaralou metodu časem zcela nahradit.

Za průkopníka v České republice by se dala pasovat České spořitelna, která už v roce 2015[39], před účinností ZoPS otevřela své API třetím stranám a umožnila jim přístup do klientských dat. Česká spořitelna pořádala v roce 2017 Open banking & WebAPI festival, na kterém proběhly workshopy, kde „účastníci hledali odpovědi na to, jak sestavovat nové aplikace, nasazovat je a snadno dosáhnout jejich vysoké dostupnosti, například při detekci anomálních transakcí na účtu.

[35] HINGAR, Petr. Otevřené bankovnictví, PSD2, open API a BankID aneb Změna paradigmatu ve finančním sektoru. *SystemOnline.cz* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://www.systemonline.cz/it-pro-banky-a-financni-organizace/otevrene-bankovnictvi-psd2-open-api-a-bankid.htm

[36] BARTÁČEK, Václav. Představení PSD2 nejen pro vývojáře. Blíží se otevřené bankovnictví? Udělejte si v tom jasno. *Zdroják.cz* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://zdrojak.cz/clanky/psd2-nejen-pro-vyvojare/

[37] Ibid.

[38] Co je to API (application programming interface)? *Topranker.cz* [online]. [cit. 2021-03-15]. Dostupné z: https://topranker.cz/slovnik/co-je-to-api-application-programming-interface/

[39] Jsou otevřená data příležitostí pro banky? Největší festival nad otevřenými daty v ČR. *Česká spořitelna* [online]. 2017 [cit. 2021-03-15]. Dostupné z: https://www.csas.cz/cs/o-nas/pro-media/tiskove-zpravy/2017/11/23-1/nejvetsi-festival-nad-otevrenymi-daty-v-cr

A nejen to, během hackathonu také vymýšleli způsob, jak platit hlasem nebo pracovat s aplikací, která by hlídala vývoj kurzu Bitcoin.“[40]

Myslím si, že pro případnou novou směrnici PSD3 by bylo velice vhodné harmonizovat open banking standardy napříč celou Evropskou unií a ulehčit tak více FinTech společnostem přístup na nové trhy členských států, jelikož samotné rozdíly mezi standardy jednotlivých států může učinit ne jeden problém programátorům a oddálit i případný vstup některých slibných služeb na další trhy členských států. V tomto ohledu si myslím, že zákonodárce byl velmi benevolentní a dal prostor tam, kde podle mého neměl.

2.3.1. Český Open banking standard

Český standard pro Open banking byl představen ke konci roku 2017 Českou bankovní asociací, která jej vypracovala. Tento standard upravuje například API rozhraní pro níže popsané služby v kapitole 2.4. a 2.5., jmenovitě služby nepřímé dání platebního příkazu, služby informování o platebním účtu.[41]

V současné době je Český standard pro Open banking ve verzi 4.1., která byla zveřejněna v listopadu 2020. Standard je v souladu s doporučeními České národní banky. Někteří členové asociace však mohou odchýlit od tohoto standardu v určitých částech.[42]

Je důležité zdůraznit, že Český standard pro Open banking je nezávazný standard, který je na bázi dobrovolnosti[43] a používají ho někteří členové České bankovní asociace. Jak zmiňuje třeba společnost Spendee, stalo se jim to, že nejmenovaná banka bez oznámení změnila strukturu v API a zapříčinilo to problémy, jak společnosti provozující aplikaci Spendee, tak i uživatelům.[44] Takové chování ze strany bank by se předešlo, kdyby byly tyto standardy harmonizovány.

2.3.2. Britský Open banking standard

Velká Británie, jako členský stát Evropské unie do února 2020, v rámci směrnice PSD2 implementovala do svého právního řádu jako všechny ostatní

---

[40] Jsou otevřená data příležitostí pro banky? Největší festival nad otevřenými daty v ČR. Česká spořitelna [online]. 2017 [cit. 2021-03-15]. Dostupné z: https://www.csas.cz/cs/o-nas/pro-media/tiskove-zpravy/2017/11/23-1/nejvetsi-festival-nad-otevrenymi-daty-v-cr

[41] Český standard pro Open banking. *Česká bankovní asociace* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/cesky-standard-pro-open-banking

[42] Ibid.

[43] SECHTER, Jakub. Jak jsou české banky s nástupem PSD2 otevřené svým klientům? *Lupa.cz* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://www.lupa.cz/clanky/jak-jsou-ceske-banky-s-nastupem-psd2-otevrene-svym-klientum/

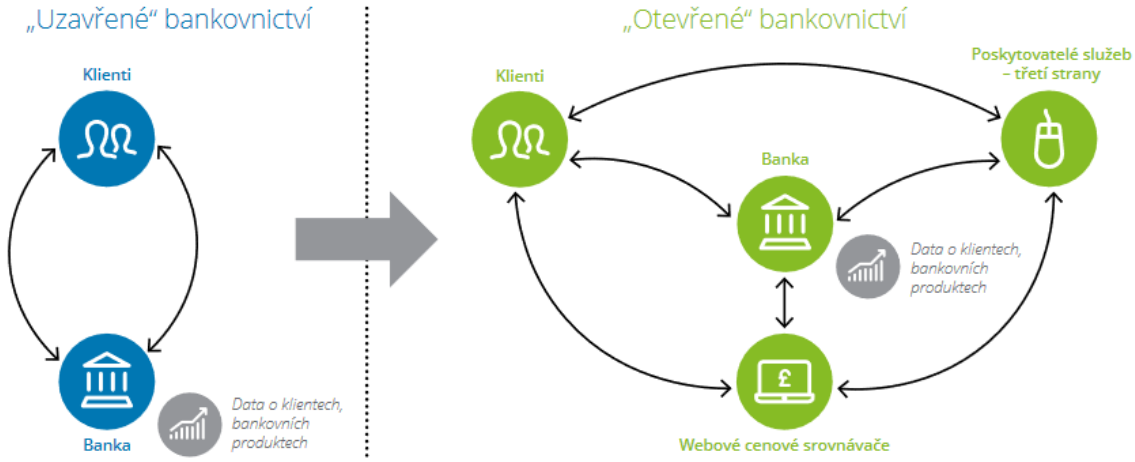
[44] Ibid.

členské státy. Myslím si, že Velká Británie může být vzorem pro ostatní členské státy Evropské unie, jak se popasovala s open banking.

Britský Open Banking je v některých věcech odlišný od kontinentálního open banking. K současné době k britskému Open Banking vstoupilo 52 bank[45], z nichž 9 největších povinně. Jiný přístup spočívá v tom, že britská Competition & Markets Authority může povolit přístup k datům klientů třetím stranám, které nemusí být regulovaným poskytovatelem platebních služeb.[46] Díky tomuto kroku můžou třeba cenové vyhledávače pomoci uživatelům vybrat výhodnější službu, přímo na míru pro klienty.[47]

Na obrázku 1 můžeme vlevo vidět klasické schéma uzavřeného bankovnictví, které bylo před zavedením směrnice PSD2 a její implementace do vnitrostátních právních řádů členských států, vpravo můžeme názorně vidět, jak funguje open banking ve Velké Británii.

Obrázek 1 *– Porovnání uzavřeného a otevřeného bankovnictví*



Upraveno ze zdroje: Jak prosperovat v nejisté době. In: *Deloitte Česká republika* [online]. 2017 [cit. 2021-03-15]. Dostupné z: https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-otevrene-bankovnictvi-a-psd2.pdf, s. 11

[45] FAQs. *Open Banking* [online]. [cit. 2021-03-15]. Dostupné z: https://www.openbanking.org.uk/customers/faqs/

[46] Jak prosperovat v nejisté době. In: *Deloitte Česká republika* [online]. 2017 [cit. 2021-03-15]. Dostupné z: https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-otevrene-bankovnictvi-a-psd2.pdf, s. 10, 11

[47] Ibid.

2.3.3. NextGenPSD2 a openFinance Framework

Posledním příkladem, který uvedu pro open banking standard, je standard z dílny iniciativy The Berlin Group, která svůj standard nazvala NextGenPSD2. Velkou výhodou tohoto standardu bylo množství účastníků, které přesáhlo přes počet 70 společností, z tohoto počtu až 75 % evropských bank.[48]

Od 1. února 2021 se NextGenPSD2 stala součástí openFinance Framework, která je novou infrastrukturou pro banky a třetí strany. Umožní poskytování dalších služeb, které směrnice PSD2 neupravuje, jako třeba platba půjčkou.[49] Dá se říct, že openFinance Framework poskytne služby, které byly zmíněny v 2.3.2. a umožní tak FinTech společnosti a další společnosti rozšířit pole působnosti, což bude pouze výhoda pro budoucí uživatele. Nutno dodat, že openFinance Framework je teprve ve fázi tržní konzultace (stav k 8. března 2021).

2.4. Služba informování o platebním účtu – AIS

Jednou z novinek směrnice PSD2, která je, troufám si tvrdit, jedním ze stěžejních pro současnou open banking platformu, je služba informování o platebním účtu. Už v úvodu kapitoly 2 jsem nastínil, že služba informování o platebním účtu může mít spoustu funkcionalit, které používáme na denní bázi. Více o praktickém využití v kapitole 2.6.

ZoPS přímo definuje službu informování o platebním účtu takto: „služba spočívající ve sdělování informací o platebním účtu prostřednictvím internetu poskytovatelem rozdílným od poskytovatele, který vede daný platební účet“[50]. Služba informování o platebním účtu je jinak známá pod anglickým termínem „Account Information Services“ nebo pod zkratkou AIS nebo ve frankofonních zemích známá jako „Le service d’information sure les comptes“. Ve směrnici PSD2 ji najdeme pod označením služba informování o účtu.

Tato služba je poskytována uživateli a je důležité zdůraznit, že nezahrnuje situace, kdy informace o platebním účtu zpřístupňují jiným osobám, například bance při posuzování úvěruschopnosti klienta například při spotřebitelském úvěru.

[48] PSD2 Access to Bank Accounts. *The Berlin Group* [online]. [cit. 2021-03-15]. Dostupné z: https://www.berlin-group.org/psd2-access-to-bank-accounts

[49] PRESS RELEASE - Berlin Group starts new openFinance API Framework. *The Berlin Group* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://www.berlin-group.org/single-post/press-release-berlin-group-starts-new-openfinance-api-framework

[50] § 2, odst. 1, písm. l) zákona č. 370/2017 Sb., o platebním styku

Pokud s tím uživatel výslovně nebude souhlasit, že takové data poskytne banka třetí straně k tomuto účelu.[51]

Informace z platebních účtů před příchodem směrnice PSD2 a implementace do právních řádů členských států Evropské unie (u nás ZoPS) se čerpaly jinými způsoby než přes API rozhraní bank. Existovaly služby, které fungovaly na bázi nahrávání dat z platebního účtu (například ve strojově čitelném formátu .csv nebo .xml), výpisů v .pdf, přístupem přes internetové bankovnictví nebo propojení aplikace s notifikačními e-maily, které zasílala banka uživateli. Šlo zejména o aplikace/služby, které se věnovaly správě financí.[52] Například služba Spendee, o které jsem psal v kapitole 2, stále dává možnost nahrání .xls, .xlsx nebo CSV souboru[53], který vygeneruje v internetovém bankovnictví na příkaz uživatele, který má zájem o zaznamenání transakcí do aplikace a nechce použít službu informování o platebním účtu.

Zajímavostí je, že zákonodárce uvedl službu informování o platebním účtu jako platební službu, která je definovaná v ustanovení § 3 ZoPS, a přitom tato služba se těžko dá nazvat jako platební službou, jelikož není „navázána na žádné převody peněžních prostředků ani platební příkazy k těmto převodům“ [54]. Lze se domnívat, že jde o snahu zjednodušit poskytovatelům služby informování o platebním účtu (*anglicky* Account Information Services Provider, neboli ve zkratce AISP) o snazší přístup na trhy v členských zemích Evropské unie s ohledem na získané povolení k činnosti od České národní banky.[55]

2.4.1. Práva a povinnosti poskytovatele, který vede platební účet

Ihned na začátku je zapotřebí si ujasnit práva a povinnosti poskytovatelů, kteří vedou platební účet uživatele, následně práva a povinnosti poskytovatelů služby informování o platebním účtu.

---

[51] STRNADEL, Dalibor, Tomáš Nýdrle. § 2 Vymezení některých pojmů. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[52] Ibid.

[53] How to import data? *Spendee Help Center* [online]. [cit. 2021-02-22]. Dostupné z: https://help.spendee.com/article/121-import-transactions

[54] NÝDRLE, Tomáš. § 192 [*Povinnosti poskytovatele služby informování o platebním účtu*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[55] NÝDRLE, Tomáš. § 191 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

Ze zákona vyplývá, že předtím než poskytovatel, který vede platební účet (typicky banka) poskytne další třetí straně informace (typicky poskytovatel služby informování o platebním účtu), které jsou jinak „přístupné uživateli prostřednictvím internetu“[56], musí získat souhlas uživatele ke sdělení informací o platebním účtu.

Důležitá je interpretace toho, co znamenají informace dostupné uživateli prostřednictvím internetu. Prostřednictvím internetu můžeme přistoupit ke svému platebnímu účtu přes mobilní aplikaci na svých chytrých telefonech nebo prostřednictvím internetového bankovnictví na webovém prohlížeči. V aplikaci nebo internetovém bankovnictví narazíme určitě na zůstatek na platebním účtu a pohyby na účtu (historie transakcí). Autoři komentáře k ZoPS se zabývají problematikou, zda patří do těchto informací rovněž nastavení trvalých příkazů nebo souhlasy s inkasem, které jsou prováděny z účtu nebo informace o přečerpání nebo informace o existenci jiného úvěrového rámce.[57] Dle mého názoru výše, informace, které uvádí autoři komentáře za příklad, patří do tohoto rámce. Musíme vzít na vědomí, jakou funkcionalitu služba informování o platebním účtu poskytuje uživatelům nebo může teoreticky poskytnout, a proto bych informace nad kterými uvažují autoři komentáře, zahrnul mezi sdílené informace, protože se mi nezdá, že by to bylo v rozporu s tím, co chtěl zákonodárce dosáhnout tímto ustanovením. Zejména v aplikacích, které spravují finance uživatelům, je záhodno započítávat platby, které mají odejít v příštím měsíci nebo o kterou částku přečerpal uživatel limit svého účtu. Správně autoři komentáře naráží na to, že každý poskytovatel platebního účtu, rozuměje banka, dává uživateli určitý okruh informací, avšak s příchodem open banking standardu si nemyslím, že je toto problém pro sdílení s třetími stranami.

Otazník visí nad tím, co znamená souhlas uživatele, o kterém referuje ustanovení § 191, odstavce 1 ZoPS a čím se uděluje tento souhlas. Jednou z možností může být obsažení daného souhlasu přímo ve smlouvě o poskytování platebních služeb, uzavřenou mezi uživatelem a poskytovatelem, který vede platební účet. Tento souhlas má být dle směrnice PSD2 výslovný, avšak v praxi tento požadavek se nevyžaduje. Souhlas by měl být směrován vůči poskytovateli,

[56] § 191, odst. 1 zákona č. 370/2017 Sb., o platebním styku

[57] NÝDRLE, Tomáš. § 191 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

který vede platební účet, ale může nastat i možnost, kdy souhlas může být dán přes poskytovatele služby informování o platebním účtu.[58]

ZoPS zdůrazňuje, že: „Poskytovatel, který uživateli vede platební účet, nesmí činit neodůvodněné rozdíly mezi žádostmi o informace o platebním účtu.“[59] Poskytovatel, který vede platební účet by tedy neměl diskriminovat a rozlišovat žádosti, které jsou přímo od uživatele (například z internetového bankovnictví) nebo prostřednictvím třetí strany, tedy nepřímo od uživatele.[60]

Poskytovatel, který vede platební účet, může ze zákonných důvodů odmítnout sdělit informace o platebním účtu poskytovateli služby informování o platebním účtu. V případě, že nastane jeden či více níže uvedených případů poskytovatel, který vede platební účet, nemusí přistoupit k odmítnutí sdělit informace poskytovateli služby informování o platebním účtu.[61] ZoPS udává následující důvody:

„a) má-li podezření na neautorizované nebo podvodné použití platebního prostředku, nebo osobních bezpečnostních prvků uživatele,

b) není-li poskytovatel, který žádá o informace, oprávněn poskytovat službu informování o platebním účtu, nebo

c) neosvědčil-li poskytovatel služby informování o platebním účtu svoji totožnost v souladu s § 192 písm. c).“[62]

Prvním důvodem je tedy „podezření na neautorizované nebo podvodné použití platebního prostředku, nebo osobních bezpečnostních prvků uživatele“.[63] Může jít o případ, kdy poskytovatel, který vede platební účet, má podezření, že přístup k informacím o platebním účtu se chce dostat neoprávněná osoba bez souhlasu uživatele.[64]

---

[58] NÝDRLE, Tomáš. § 191 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[59] § 191, odst. 2 zákona č. 370/2017 Sb., o platebním styku

[60] NÝDRLE, Tomáš. § 191 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[61] Ibid.

[62] § 191, odst. 3 zákona č. 370/2017 Sb., o platebním styku

[63] Ibid.

[64] NÝDRLE, Tomáš. § 191 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

Dalším důvodem, kdy může poskytovatel, který vede platební účet odmítnout sdělit informace je tehdy, když poskytovatel, který žádá informace nemá oprávnění danou službu poskytovat.

Na základě povolení k poskytování platebních služeb mohou banky a spořitelní a úvěrní družstva poskytovat tuto službu jako platební instituce. Platební instituce nebo instituce elektronických peněz musí mít službu informování o platebním účtu přímo uvedenou v povolení k činnosti nebo správci informací o platebním účtu, kteří získali povolení k činnosti.[65] Takoví poskytovatelé se nazývají správci informací o platebním účtu. Seznam těchto poskytovatelů je dostupný na stránkách České národní banky.

Poslední důvod nastane v případě, pokud poskytovatel služby informování o platebním účtu neosvědčí totožnost „při každém dotazu na informace o platebním účtu“.[66] Pro takovou identifikaci „využívají poskytovatelé služby informování o platebním účtu kvalifikované certifikáty pro elektronické pečetě (srov. čl. 3 bodu 30 nařízení eIDAS) nebo kvalifikované certifikáty pro autentizaci internetových stránek (srov. čl. 3 bodu 39 nařízení eIDAS)“[67].

Pokud nastane jeden z výše uvedených scénářů, poskytovatel, který vede platební účet, musí informovat uživatele o takové skutečnosti bez zbytečného odkladu. Jelikož pro přístup k těmto informacím na platebním účtu uživatele využívá v dnešní době API rozhraní, dle komentáře k ZoPS bude spíše docházet ke scénáři, kdy bude uživatel informován o odmítnutí sdělení informací poskytovateli služby informování o platebním účtu ex-post.[68] Z toho důvodu, že informace „jsou poskytovány ve velmi krátkém čase po obdržení žádosti uživatele či třetí strany jednající jménem uživatele“.[69]

Tímto ale nekončí informační povinnost poskytovatele, který vede platební účet, jelikož informační povinnost se netýká pouze uživatele, kterému vede platební

---

[65] NÝDRLE, Tomáš. § 191 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[66] § 192, písm. c) zákona č. 370/2017 Sb., o platebním styku

[67] NÝDRLE, Tomáš. § 192 [*Povinnosti poskytovatele služby informování o platebním účtu*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[68] NÝDRLE, Tomáš. § 191 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[69] Ibid.

účet, ale musí informovat bez zbytečného odkladu i Českou národní banku, která vydává povolení k činnosti těmto uživatelům a vykonává nad nimi dohled.

2.4.2. Požadavky pro poskytnutí služby informací o platebním účtu

Poskytovatel služby informování o platebním účtu má ze zákona povinnosti, které musí dodržet při poskytování dané služby. Možná se někteří mohou divit, proč tato skutečnost není uvedena v ZoPS jako požadavek pro správce informací o platebním účtu, ale nesmíme zapomenout na výše uvedená fakta v kapitole 2.4.1., že službu informování o platebním účtu můžou poskytovat jak správci informací o platebním účtu, kteří získali povolení k činnosti od České národní banky za účelem poskytnutí této služby, tak ale i banky a spořitelní a úvěrní družstva mají možnost poskytovat tuto službu dle povolení k poskytování platebních služeb. Mezi požadavky pro poskytovatele patří:

„a) poskytuje službu informování o platebním účtu na základě výslovného souhlasu, který mu uživatel udělil,

b) zpřístupní osobní bezpečnostní prvky uživatele pouze uživateli a tomu, kdo je vydal,

c) při každém dotazu na informace o platebním účtu osvědčí poskytovateli, který uživateli vede platební účet, svoji totožnost,

d) v souvislosti se službou informování o platebním účtu získává a zpracovává pouze informace o platebním účtu, který určil uživatel,

e) nepožaduje citlivé údaje o platbách uživatele a

f) v souvislosti se službou informování o platebním účtu nepožaduje od uživatele, neuchovává a nezpracovává jiné údaje o uživateli, nebo jeho platebním účtu než údaje potřebné k poskytnutí služby informování o platebním účtu.“[70]

Uživatel musí dát souhlas i poskytovateli služby informování o platebním účtu, neliší se to tedy od souhlasu poskytovateli, který vede platební účet. V tomto případě se dává souhlas uživatel poskytovateli služby informování o platebním účtu tím, že se uzavře smlouva o platebních službách s tímto poskytovatelem. Každých 90 dnů musí proběhnout silné ověření uživatele, během kterého musí uživatel dát souhlas s tím, aby byly dále poskytovány údaje z platebního účtu tomuto poskytovateli služby informování o platebním účtu.[71]

---

[70] § 192 zákona č. 370/2017 Sb., o platebním styku

[71] NÝDRLE, Tomáš. § 192 [*Povinnosti poskytovatele služby informování o platebním účtu*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

Dalším požadavkem pro zpřístupnění jsou „osobní bezpečnostní prvky uživatele pouze uživateli a tomu, kdo je vydal“[72]. Co je osobní bezpečnostní prvek? Takovým prvkem se rozumí „prvek, který poskytovatel poskytl uživateli za účelem ověření“.[73]

Požadavkem osvědčení totožnosti poskytovatele „pro účely identifikace poskytovatelů se využívají kvalifikované certifikáty pro elektronické pečetě (srov. čl. 3 bodu 30 nařízení eIDAS) nebo kvalifikované certifikáty pro autentizaci internetových stránek (srov. čl. 3 bodu 39 nařízení eIDAS)“.[74]

Poskytovatel služby informování o platebním účtu může získat a zpracovávat pouze ty informace, které uživatel povolí. Myslím si, že je to správný krok, i kvůli tomu, že uživatel může nabýt pocitu, že v dnešním světě má šanci stále ovlivňovat data, která proudí internetem. Já osobně v současné době nevyužívám službu informování o platebním účtu, a kdybych se k tomu někdy uchýlil, nemyslím si, že budu potřebovat více než zůstatek na mém druhém bankovním účtu. S aplikací, která by mi spravovala finance, bych mohl nabýt jiného názoru, ale nemyslím si, že někdy takovou aplikaci využiji. Zejména s ohledem na můj skeptický pocit, že dávám své finanční údaje třetí straně.

Citlivým údajem o platbách uživatele se rozumí „údaj, který může být zneužit k podvodu v oblasti platebních služeb, s výjimkou jedinečného identifikátoru a jména majitele platebního účtu v případě poskytovatele služby informování o platebním účtu nebo služby nepřímého dání platebního příkazu“.[75] V praxi to znamená podle komentáře k ZoPS, že poskytovatel služby informování o platebním účtu nemá možnost přistupovat k účtu prostřednictvím uživatelského rozhraní[76].

Posledním požadavkem je, že poskytovatel služby informování o platebním účtu nesmí uchovávat, zpracovávat ani vyžadovat jiné údaje, které nejsou potřebné k poskytnutí dané služby[77].

---

[72] § 192, písm. b) zákona č. 370/2017 Sb., o platebním styku

[73] § 2, odst. 3, písm. m) zákona č. 370/2017 Sb., o platebním styku

[74] NÝDRLE, Tomáš. § 192 [*Povinnosti poskytovatele služby informování o platebním účtu*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[75] § 2, odst. 3, písm. n) zákona č. 370/2017 Sb., o platebním styku

[76] NÝDRLE, Tomáš. § 192 [*Povinnosti poskytovatele služby informování o platebním účtu*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[77] § 192, písm. f) zákona č. 370/2017 Sb., o platebním styku

Nelze však opomenout povinnost z ustanovení § 49, odst. 1 ZoPS, který zavádí informační povinnost a uchovávání dokumentů a záznamů.

Informační povinnost poskytovatele zahrnuje zejména: „finanční situaci, výsledcích svého hospodaření, plnění podmínek výkonu své činnosti“[78]. Vyhláška č. 454/2017 Sb., o informačních povinnostech některých osob oprávněných poskytovat platební služby nebo vydávat elektronické peníze stanoví podrobnější výkazy, které musí správce informací o platebním účtu sestavovat. Jedná se například o čtvrtletní rozvahu[79] a čtvrtletní výkaz zisku a ztráty[80].

Ohledně uchovávání dokumentů a záznamů, které se týkají plnění povinností se musí uchovávat „alespoň po dobu 5 let ode dne, kdy tyto dokumenty nebo záznamy vznikly“[81].

2.4.3. Povolení k činnosti pro správce informací o platebním účtu od České národní banky

V kapitole 2.4.1. se zmiňuji o tom, že banky, spořitelní a úvěrní družstva mohou jako poskytovatelé platebních služeb poskytovat službu informování o platebním účtu, avšak mezi poskytovatele se mohou zařadit i další, a to správci informací o platebním účtu.

ZoPS definuje správce informací o platebním účtu jako toho, „kdo je oprávněn poskytovat službu informování o platebním účtu na základě povolení k činnosti správce informací o platebním účtu, které mu udělila Česká národní banka.“[82]

Žádost žadatel podává elektronicky, musí splnit podmínky (viz kapitola 2.4.3.1.), které žadatel doloží potřebnou dokumentací.[83] Tato žádost musí splňovat náležitosti zákona č. 500/2004 Sb., správní řád, který ustanovení § 37 a náležitosti z vyhlášky č. 1/2018 Sb., o žádostech a oznámeních k výkonu činnosti podle zákona o platebním styku, konkrétně ustanovení § 6, mezi kterými zahrnuje například zakladatelské právní jednání. V souvislosti s podáním žádosti platí žadatel správní

[78] § 30, odst. 1 zákona č. 370/2017 Sb., o platebním styku

[79] § 4, odst. 4, písm. a) vyhlášky č. Vyhláška č. 454/2017 Sb., o informačních povinnostech některých osob oprávněných poskytovat platební služby nebo vydávat elektronické peníze

[80] Ibid.

[81] § 31, odst. 1 zákona č. 370/2017 Sb., o platebním styku

[82] § 41 Ibid.

[83] § 43, odst. 1 Ibid.

poplatek, který je dán zákonem č. 634/2004 Sb., o správních poplatcích, který udává částku 25 000 Kč[84].

V případě, že se v žádosti změní údaje nebo přílohy, musí žadatel nebo správce informací o platebním účtu (pokud už má povolení k činnosti) oznámit bez zbytečného odkladu České národní bance.[85]

Česká národní banka dle ZoPS má povinnost do 3 měsíců od zahájení řízení vydat rozhodnutí, avšak v případě neúplnosti žádosti nebo podstatných vad, které brání v pokračování řízení, lhůta běží ode dne odstranění.[86] V médiích proběhly zprávy, kdy si první subjekt s tímto povolením stěžoval, že proces trval dlouho, a tak přišel o konkurenční náskok.[87]

Nutno dodat, že správce informací o platebním účtu může poskytovat pouze danou službu a žádnou další platební službu.[88]

2.4.3.1. Podmínky pro žadatele

Důležité je na začátku zmínit, že správcem se může stát jak právnická osoba, tak i fyzická osoba.[89] K tomu, aby se žadatel mohl stát správcem informací o platebním účtu, musí splnit následující zákonné podmínky:

„a) který má sídlo i skutečné sídlo v České republice,

b) jehož obchodní plán, včetně předpokládaného rozpočtu na první 3 účetní období, je podložen reálnými ekonomickými propočty,

c) v jehož prospěch je uzavřena pojistná smlouva nebo poskytnuto srovnatelné zajištění v souladu s tímto zákonem,

d) jehož věcné, technické, personální a organizační předpoklady jsou vhodné z hlediska řádného a obezřetného poskytování služby informování o platebním účtu,

e) jehož řídicí a kontrolní systém splňuje požadavky stanovené tímto zákonem,

f) jehož vedoucí osoby jsou důvěryhodné z hlediska řádného a obezřetného poskytování služby informování o platebním účtu,

---

[84] Příloha [Sazebník], ČÁST IV, položka 65, písm. p) zákona č. 634/2004 Sb., o správních poplatcích

[85] § 44, odst. 1 zákona č. 370/2017 Sb., o platebním styku

[86] § 43, odst 2 Ibid.

[87] BEDRICH, Vaclav. Český fintech Spendee získal od ČNB jako první licenci k přímému propojení s bankami. *CzechCrunch* [online]. 2018 [cit. 2021-03-09]. Dostupné z: https://www.czechcrunch.cz/2018/12/cesky-fintech-spendee-ziskal-od-cnb-jako-prvni-licenci-k-primemu-propojeni-s-bankami/

[88] § 49, odst. 2 zákona č. 370/2017 Sb., o platebním styku

[89] BERAN, Jiří. § 41 [*Správce informací o platebním účtu*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

g) jehož vedoucí osoby v oblasti poskytování služby informování o platebním účtu jsou odborně způsobilé a mají dostatečné zkušenosti z hlediska řádného a obezřetného poskytování služby informování o platebním účtu,
h) u něhož nenastala skutečnost, která zakládá překážku provozování živnosti podle zákona upravujícího živnostenské podnikání, a
i) který, je-li fyzickou osobou, splňuje všeobecné podmínky provozování živnosti podle zákona upravujícího živnostenské podnikání.“[90]

Jak komentář k ZoPS připomíná, podmínky jsou vcelku podobné těm, které jsou dané pro povolení k činnosti platební instituce.[91]

První podmínkou ZoPS je to, aby žadatel měl sídlo a skutečné sídlo na území České republiky. Definici sídla nalezneme v Občanském zákoníku, kdy se sídlo podnikatele „určí adresou zapsanou ve veřejném rejstříku“[92]. Veřejným rejstříkem rozumíme dle zákona o veřejných rejstřících právnických a fyzických osob: „spolkový rejstřík, nadační rejstřík, rejstřík ústavů, rejstřík společenství vlastníků jednotek, obchodní rejstřík a rejstřík obecně prospěšných společností.“[93] Sídlem rozumím tedy adresu, kterou můžeme naleznout třeba u právnické osoby v obchodním rejstříku. Skutečné sídlo je místo „odkud daný podnikatel řídí své obchodní aktivity (NS 29 Cdo 1953/2013), kde je místo správy společnosti (NS 29 Cdo 1680/2009, 29 Cdo 4993/2008), kde se veřejnost může s podnikatelem stýkat (srov. § 19c odst. 2 ObčZ 1964 ve znění účinném do 19. 7. 2009).“[94]

Neméně důležitou podmínkou je obchodní plán žadatele spolu s rozpočtem na první tři účetní období. Obchodní plán je definován ve vyhlášce č. 1/2018 Sb., o žádostech a oznámeních k výkonu činnosti podle zákona o platebním styku. Obchodní plán zahrnuje, kromě komentáře, následující:
„1. popis činnosti, z kterého vyplývá, že daná činnost naplňuje znaky služby informování o platebním účtu,
2. popis způsobu poskytování činnosti podle bodu 1 a činností s tím souvisejících, které hodlá žadatel poskytovat, se zohledněním individuálních podmínek žadatele

[90] § 42, odst. 1 zákona č. 370/2017 Sb., o platebním styku
[91] BERAN, Jiří. § 42 [*Podmínky pro udělení povolení k činnosti správce informací o platebním účtu*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.
[92] § 429, odst. 1 zákona č. 89/2012 Sb., občanský zákoník
[93] § 1, odst. 1 zákona č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob
[94] ZAPLETAL, Jiří. § 429 [*Sídlo podnikatele*]. In: PETROV, Jan, Michal VÝTISK, Vladimír BERAN. Občanský zákoník: komentář. 2. vydání. V Praze: *C.H. Beck*, 2019. Beckova edice komentované zákony. ISBN 978-80-7400-747-7.. ISBN 978-80-7400-747-7, s. 461.

a podmínek a pravidel poskytování služby informování o platebním účtu včetně doby zpracování,
3. prohlášení žadatele, že žadateli nebudou svěřovány peněžní prostředky uživatelů,
4. návrh smlouvy mezi zainteresovanými stranami související s poskytovanou službou informování o platebním účtu,
5. předpokládaný počet pracovníků v rozdělení na příslušné organizační útvary,
6. popis zamýšleného využívání pověřených zástupců a poboček nebo zajišťování činnosti jinými osobami a
7. návrh vzorové smlouvy mezi správcem informací o platebním účtu a osobou, které bude svěřen výkon provozních činností, pokud žadatel hodlá převést některou provozní činnost na jinou osobu“[95].

V návaznosti na obchodní plán je podmínka věcných, technických, personálních a organizačních předpokladů[96], které se posuzují právě v návaznosti na obchodní plán, který předkládá žadatel České národní bance. Obchodní plán má obsahovat plán, jak zajistí právě tyto předpoklady, které by měly být v souladu s řádným a obezřetným poskytováním této služby.[97]

Žadatel musí uzavřít pojistnou smlouvu nebo zajištění, které stanoví ustanovení § 46 ZoPS. Povinnost uzavřít pojišťovací smlouvu nebo mít dostatečné zajištění vyplývá z toho, že správci informací o platebním účtu nemusí splňovat kapitálové požadavky z důvodu nepřijetí peněžních prostředků[98]. Pojistná smlouva nebo zajištění má zajistit právo na plnění, pokud správce informací o platebním účtu neoprávněně získá nebo užije informaci o platebním účtu. Vyhláška č. 7/2018 Sb., o některých podmínkách výkonu činnosti platební instituce, správce informací o platebním účtu, poskytovatele platebních služeb malého rozsahu, instituce elektronických peněz a vydavatele elektronických peněz malého rozsahu stanoví minimální limit pojistného plnění a minimální výši zajištění, který je daný v závislosti na:
„a) rizika, kterým je nebo může být správce informací o platebním účtu vystaven,
b) jiné činnosti správce informací o platebním účtu,

[95] § 6, odst. 3, písm. a) vyhlášky č. 1/2018 Sb., o žádostech a oznámeních k výkonu činnosti podle zákona o platebním styku
[96] § 42, odst. 1, písm. e) zákona č. 370/2017 Sb., o platebním styku
[97] BERAN, Jiří. § 9 [*Podmínky pro udělení povolení k činnosti platební instituce*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.
[98] Důvodová zpráva k zákonu č. 370/2017 Sb. o platebním styku, č. 370/2017 Dz

c) vlastnosti srovnatelného zajištění a

d) počet uživatelů služby informování o platebním účtu.“[99]

Řídící a kontrolní systém žadatele musí splnit požadavky, které ZoPS udává v ustanovení § 47, což znamená, že musí vykonávat správu řádně a obezřetně. Tento výklad se dá vyložit jako ustanovení § 19 ZoPS, které nastavuje stejnou povinnost platební instituci. Řádný výkon se dá vyložit jako výkon činnosti „v souladu s požadavky vyplývajícími z právních předpisů“[100], který je dle autorů komentáře k ZoPS vůdčím principem než povinnost. Obezřetný výkon je zejména minimalizace rizik, vůči kterým správce může být vystaven[101]. Řídící a kontrolní systém je „soubor zásad a postupů“[102], která by měla obsahovat ve vnitřních předpisech žadatele. Předpoklady jsou obsaženy ve vyhlášce č. 7/2018 Sb., o některých podmínkách výkonu činnosti platební instituce, správce informací o platebním účtu, poskytovatele platebních služeb malého rozsahu, instituce elektronických peněz a vydavatele elektronických peněz malého rozsahu.

Vedoucí osoby by měli být důvěryhodné, odborně způsobilé a mít dostatečné zkušenosti. ZoPS udává, že „za důvěryhodnou považuje osoba, jejíž dosavadní činnost dává předpoklad řádného výkonu činnosti“[103]. Česká národní banka ve svém výkladu udává, že obecnými kritériem je dodržování právních a etických pravidel, morálního profilu a integrity. České národní banka posuzuje i její bezúhonnost. K posouzení používá podklady z veřejně dostupných zdrojů, vlastního zjištění a z podkladů od posuzované osoby[104].

Odbornou způsobilost zkoumá Česká národní banka dle znalostí, odborné praxe na finančním trhu, manažerské praxe a z dosavadního působení na finančním trhu, kterou posuzuje taktéž z výše uvedených zdrojů, jako u důvěryhodnosti.[105]

Mezi posledními podmínkami z tohoto výčtu patří:

a) požadavek, aby nenastala překážka provozování živnosti, kterou ze ZoPS odkazuje na zákon č. 455/1991 Sb., o živnostenském podnikání, který v ustanovení

[99] § 46, odst. 2 zákona č. 370/2017 Sb., o platebním styku

[100] BERAN, Jiří. § 19 [*Řádný a obezřetný výkon činnosti platební instituce*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[101] Ibid.

[102] Ibid.

[103] § 261 zákona č. 370/2017 Sb., o platebním styku

[104] Úřední sdělení České národní banky č. 18/2020 Věst. ČNB ze dne 5. srpna 2020 k výkladu pojmů důvěryhodnost a odborná způsobilost

[105] Ibid.

§ 8 poskytuje výčet překážek provozování živnosti, zejména v souvislosti s prohlášením konkurzu na majetek fyzické či právnické osoby nebo insolvenčním řízením, a

b) v případě fyzické osoby, aby splňovala „všeobecné podmínky provozování živnosti“[106], což znamená opět exkurz do zákona č. 455/1991 Sb., o živnostenském podnikání, který v ustanovení § 6 stanoví plnou svéprávnost a bezúhonnost.

2.4.3.2. Zánik povolení k činnosti

Zánik povolení k činnosti od České národní banky může nastat z následujících důvodů:

„a) smrti nebo zrušení správce informací o platebním účtu,

b) nabytí právní moci rozhodnutí o úpadku správce informací o platebním účtu,

c) vykonatelnosti rozhodnutí, kterým Česká národní banka udělila správci informací o platebním účtu povolení k činnosti platební instituce nebo povolení k činnosti instituce elektronických peněz, nebo

d) nabytí vykonatelnosti rozhodnutí o odnětí povolení k činnosti správce informací o platebním účtu.“[107]

2.4.4. Správci informací o platebním účtu v České republice

Vzhledem k tomu, že účinnost ZoPS je od 1. ledna 2018, na trhu se už vyskytli někteří správci informací o platebním účtu, kteří zdárně prošli řízením o žádosti o udělení povolení k činnosti a splnili všechny předpoklady dané ZoPS a souvisejícími prováděcími vyhláškami. Seznam těchto správců je volně dostupný na stránkách České národní banky. Každý uživatel, který má zájem použít službu informování o platebním účtu si může prověřit, zda poskytovatel má povolení k činnosti.

V současné době pouze tři právnické osoby získaly povolení k činnosti a to:

a) SPENDEE a.s.,

b) BudgetBakers s.r.o., a

c) 1. PF Finance, s.r.o.[108]

Společnost SPENDEE a.s., IČO: 059 12 890, se sídlem náměstí I. P. Pavlova 1789/5, Nové Město, 120 00 Praha 2, Česká republika byla první

---

[106] § 42, odst. 1, písm. i) zákona č. 370/2017 Sb., o platebním styku

[107] § 45 Ibid.

[108] Správci informací o platebním účtu a pobočky zahraničních správců informací o platebním účtu (stav ke dni 02.03.2021). *Základní seznamy subjektů (výsledné sestavy)* [online]. [cit. 2021-03-02]. Dostupné z: https://apl.cnb.cz/apljerrsdad/JERRS.WEB15.BASIC_LISTINGS_RESPONSE_3?p_lang=cz&p_DATUM=02.03.2021&p_hie=HI&p_rec_per_page=25&p_ses_idx=355

společností, která získala povolení k činnosti jako správce informací o platebním účtu. Oprávněním k činnosti disponuje od 28. prosince 2018. Tato společnost provozuje aplikaci Spendee, kterou rozeberu více v kapitole 2.6.2.

Společnost BugetBakers s.r.o., IČO: 028 82 957, se sídlem Radlická 180/50, Smíchov, 150 00 Praha 5, Česká republika, byla další společností, která získala oprávnění k činnosti od 12. prosince 2019. Provozuje aplikaci Wallet, která bude zmíněna více též v kapitole 2.6.2.

Zatím poslední společností, která získala povolení k činnosti správce informování o platebním účtu k 29. července 2020, se stala společnost 1. PF Finance, s.r.o., IČO: 093 73 292, se sídlem Služská 1865/15, Kobylisy, 182 00 Praha 8, Česká republika. Společnost poskytuje ohodnocení bonity žadatele půjčky. Více v kapitole 2.6.3.

2.5. Služba nepřímé dání platebního příkazu – PIS

Další novou platební službou vycházející ze směrnice PSD2 je služba nepřímého dání platebního příkazu, která se využívá nejviditelněji v multibanking aplikacích. Službu nepřímého dání platebního příkazu zařazuji mezi zásadní novinky ze směrnice PSD2, potažmo ZoPS, jelikož se může stát velice žádanou alternativou k platbě kartou[109], například při nakupování na internetových na e shopech. Výhodou této služby je, že při využití této služby nemusí prodejce hradit poplatek ve výši několika procent z prodejní ceny karetní asociaci (například VISA, Mastercard).

Na začátek musím podotknout, že jsem s příchodem směrnice PSD2 čekal, že služba nepřímé dání platebního příkazu bude žádanou službou a vítanou alternativou k platbě kartou v e-commerce oblasti, ale realita je značně odlišná. Například ve Velké Brátnii, za období od ledna 2018 do dubna 2019, získalo povolení pro poskytování služby informování o platebním účtu 80 poskytovatelů a jenom 30 poskytovatelů získalo povolení k činnosti služby nepřímého dání platebního příkazu.[110]

V České republice službu nepřímého dání platebního příkazu „mohou poskytovat pouze banky, družstevní záložny, platební instituce nebo instituce

[109] Důvodová zpráva k zákonu č. 370/2017 Sb. o platebním styku, č. 370/2017 Dz

[110] AIS and PIS – A status update on open banking licenses issued in the UK. *Penser* [online]. 05.2019n. l. [cit. 2021-03-07]. Dostupné z: https://www.penser.co.uk/business/ais-and-pis-a-status-update-on-the-licenses-issued-in-the-uk/

elektronických peněz“[111]. Je zapotřebí zmínit, že platební instituce a instituce elektronických peněz musí rozšířit povolení k činnosti o danou službu, zatímco banky a družstevní záložny nemusí.[112]

I tato služba, jako u služby informování o platebním účtu, předběhla legislativu, a služby na podobné bázi už fungovaly před příchodem evropské legislativy, potažmo české. Tyto služby třetích stran fungovaly buď na principu screen scrapingu či přesměrování.[113]

Na základě přesměrování fungovala služba iDEAL z Nizozemska, která přesměrovala plátce při volbě dané platební metody do jeho internetového bankovnictví. Tam plátce pouze potvrdil platební příkaz, který byl předvyplněný dle obchodníka a následně banka obchodníka informovala obchodníka, že byla platba provedena. Fungoval tu vztah plátce, plátcova banka, obchodník a banka obchodníka, kdy iDEAL měla za úkol technickou komunikaci mezi bankami.[114]

Přes screen scraping, jinak řečeno uživatelské rozhraní, sdílel plátce své přístupové údaje třetí straně, která potom přistoupila do plátcova internetového bankovnictví a zadal příkaz k úhradě.[115]

Službu nepřímého dání platebního příkazu můžeme najít pod dalšími termíny, jako Payment Initation Service (anglicky), PIS nebo ve směrnici PSD2 ji najdeme pod názvem služba iniciování platby. Nejvíc zažitá je zkratka PIS, na základě mého úsudku z rešerše na dané téma.

Služba nepřímé dání platebního příkazu je v ZoPS definována, jako „služba spočívající v dání platebního příkazu k převodu peněžních prostředků z platebního účtu jménem plátce poskytovatelem rozdílným od poskytovatele, který pro plátce vede daný platební účet, je-li platební příkaz dán prostřednictvím internetu“.[116]

Principiálně to funguje tak, že v této službě figurují tři subjekty. Plátce, poskytovatel, který vede platební účet a poskytovatel nepřímého dání platebního příkazu, který se v literatuře nazývá většinou jako TPP, tedy Third Party Provider

[111] MOSNÁKOVÁ, Michaela. PSD2 a nová platební služba: Nepřímé udělení platebního příkazu. *Epravo.cz* [online]. 2018 [cit. 2021-03-06]. Dostupné z: https://www.epravo.cz/top/clanky/psd2-a-nova-platebni-sluzba-neprime-udeleni-platebniho-prikazu-107127.html

[112] Ibid.

[113] NÝDRLE, Tomáš. § 161 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[114] Ibid.

[115] Ibid.

[116] § 2, odst. 1, písm. k) zákona č. 370/2017 Sb., o platebním styku

nebo třetí strana. Plátce prostřednictvím poskytovateli nepřímého dání platebního příkazu zadá platební příkaz, kterou třetí strana předá poskytovateli, který vede platební účet. Je důležité zmínit, že příkaz, který předává poskytovatel nepřímého dání platebního příkazu poskytovateli, který vede plátci platební účet je stále příkaz k platbě, který zadal plátce, a tady můžeme spatřit prvek nepřímosti, jelikož příkaz zadal u poskytovatele nepřímé dání platebního příkazu.[117]

Způsob dání souhlasu a příkazu plátce poskytovateli nepřímého dání platebního příkazu si dohodnou mezi sebou. Poskytovatel, který vede platební účet plátci má pouze vytvořit platformu k tomu, aby jej poskytovatel nepřímého dání platebního příkazu mohl předat.[118]

2.5.1. Práva a povinnosti poskytovatele, který vede platební účet

Poskytovatel, který vede platební účet plátci dle ZoPS má povinnosti, které musí dodržet v případě, že plátce zadá nepřímo platební příkaz přes poskytovatele nepřímého dání platebního příkazu.

Jedna z povinností poskytovatele, který vede platební účet plátci, je ta, že po přijetí tohoto nepřímého platebního příkazu musí sdělit dostupné informace o přijetí a provedení platební transakce. Otázkou je, co znamenají dostupné informace o přijetí nepřímo daného platebního příkazu. Autoři komentáře k ZoPS si myslí, že nejde o sdělení, zda proběhne tato platební transakce, ale mezi informace se řadí to, zda na plátcově platebním účtu je dostatek zůstatku na účtu pro provedení této platební transakce[119]. Provedení samotné platební transakce může zmařit fakt, že poskytovatel, který vede platební účet plátci, může odmítnout transakci z následujících důvodů:

„a) má-li podezření na neoprávněné nebo podvodné použití platebního prostředku nebo osobních bezpečnostních prvků uživatele,

b) byl-li platební příkaz nepřímo dán prostřednictvím osoby, která není oprávněna poskytovat službu nepřímého dání platebního příkazu,

c) neosvědčil-li poskytovatel nepřímého dání platebního příkazu svoji totožnost v souladu s § 162 písm. e), nebo

d) jsou-li splněny podmínky podle § 159 odst. 1.“[120]

---

[117] NÝDRLE, Tomáš. § 161 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[118] Ibid.

[119] Ibid.

[120] § 161, odst. 3 zákona č. 370/2017 Sb., o platebním styku

Pokud má poskytovatel, který vede platební účet plátci, „podezření na neoprávněné nebo podvodné použití platebního prostředku nebo osobních bezpečnostních prvků uživatele“[121], může platební transakci odmítnout. Taková situace může nastat v případě, že platební příkaz zadá jiná osoba než plátce nebo jím zmocněná osoba. S ohledem na osobní bezpečnostní prvky, které jsou v ustanovení § 161, odst. 3, písm a) ZoPS se rozumí i případ, kdy se do rozhraní plátce přihlásí jiná osoba než on sám.[122]

Další případ může nastat tehdy, pokud je nepřímý platební příkaz je dán u osoby, která nemá oprávnění poskytovat tuto službu. Jak jsem zmiňoval v kapitole 2.5., k poskytování této služby jsou oprávněni: „banky, družstevní záložny, platební instituce nebo instituce elektronických peněz“.[123] Z toho vyplývá, že mimo tento okruh, s výjimkou platebních institucí a institucí elektronických peněz, bez povolení k službě nepřímého dání platebního příkazu, nemůže tuto službu poskytovat nikdo jiný a je to důvod k odmítnutí takového příkazu.

I u služby nepřímého dání platebního příkazu, má poskytovatel, který vede platební účet, právo k osvědčení totožnosti poskytovatele služby nepřímého dání platebního příkazu. Ani v tomto případě se nepostupuje jinak a k ověření totožnosti se „využívají kvalifikované certifikáty pro elektronické pečetě (srov. čl. 3 bodu 30 nařízení eIDAS) nebo kvalifikované certifikáty pro autentizaci internetových stránek (srov. čl. 3 bodu 39 nařízení eIDAS)“[124].

Pokud nastane odmítnutí transakce na základě výše uvedených 3 případů, musí to bez zbytečného odkladu nahlásit poskytovatel, který vede platební účet České národní bance, která provádí dohled nad finančním trhem. Dle komentáře k ZoPS je taková povinnost snahou odradit poskytovatele od neodůvodněných odmítnutí nepřímo daných platebních příkazů.[125] Což se dá vyložit i tímto způsobem, avšak Česká národní banka jako orgán vykonávající dohled by měla mít

[121] § 161, odst. 3, písm. a) Ibid.

[122] NÝDRLE, Tomáš. § 161 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[123] MOSNÁKOVÁ, Michaela. PSD2 a nová platební služba: Nepřímé udělení platebního příkazu. *Epravo.cz* [online]. 2018 [cit. 2021-03-06]. Dostupné z: https://www.epravo.cz/top/clanky/psd2-a-nova-platebni-sluzba-neprime-udeleni-platebniho-prikazu-107127.html

[124] NÝDRLE, Tomáš. § 161 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[125] Ibid.

přehled celkově o takových pochybnostech, navíc přímo směrnice PSD2 v ustanovení článku 68, odst. 6 takové jednání požaduje.[126]

Posledním případem, kdy může poskytovatel, který vede platební účet plátce, odmítnout transakci, je důvod z ustanovení § 159 odst. 1 ZoPS, který zní následovně: „Poskytovatel může platební příkaz odmítnout, jestliže není povinen platební transakci provést. Poskytovatel služby nepřímého dání platebního příkazu může platební příkaz odmítnout, jestliže není povinen nepřímo daný platební příkaz předat poskytovateli vedoucímu platební účet.“[127] Komentář k ZoPS uvádí příklad, kdy má poskytovatel, který vede platební účet, stanovit s uživatelem (budoucím plátcem) důvody a situace, kdy nebude povinen provést platební transakci.[128]

V případě, že poskytovatel, který vede platební účet plátci chce z výše uvedených důvodů odmítnout nepřímo daný platební příkaz, „informuje uživatele o důvodech odmítnutí; není-li to možné, informuje uživatele bez zbytečného odkladu po odmítnutí“[129]. To znamená, že před tím, než učiní samotné odmítnutí, musí informovat plátce o tomto úmyslu se zdůvodněním, proč tak chce učinit. Povinnost informovat o tomto úmyslu odpadá, pokud by to ohrozilo bezpečnost v oblasti platebního styku.[130]

ZoPS udává dále povinnost poskytovateli v ustanovení § 161, odst. 1, písm. b), že: „nesmí při přijetí nebo odmítnutí platebního příkazu činit neodůvodněné rozdíly mezi nepřímo daným platebním příkazem a ostatními platebními příkazy; to platí i pro provedení související platební transakce“[131]. Poskytovatel, který vede platební účet plátci by neměl diskriminovat nepřímo daný platební příkaz v porovnání s ostatními platebními příkazy, což je logické, jelikož nepřímé dání platebního příkazu měla být alternativou platbě kartou. Komentář k ZoPS hovoří, že zvýhodnění by mohlo být: „stanovením rozdílné lhůty pro provedení platební

[126] NÝDRLE, Tomáš. § 161 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[127] § 159, odst. 1 zákona č. 370/2017 Sb., o platebním styku

[128] NÝDRLE, Tomáš. § 161 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[129] § 161, odst. 4 zákona č. 370/2017 Sb., o platebním styku

[130] NÝDRLE, Tomáš. § 161 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[131] § 161, odst. 1, písm. b) zákona č. 370/2017 Sb., o platebním styku

transakce, ke které byl dán platební příkaz nepřímo, oproti platebním transakcím, kde byl dán platební příkaz přímo. Zakázána je pak zjevně i diskriminace v reálné lhůtě provádění platebních transakcí. Nestačí tedy jen deklarovat stejné lhůty, ale tyto lhůty je třeba dodržovat.“[132]

Poskytovatel, který vede platební účet, musí umožnit přijetí nepřímo daného platebního příkazu všem poskytovatelům této služby a nesmí podmiňovat přijetí nepřímého platebního příkazu tím, že by poskytovatel této služby měl mít uzavřenou smlouvu s ním. Domnívám se, že v případě nezavedení této podmínky v ZoPS, by se mohlo stát, že poskytovatelé, kteří vedou platební účet mohou danou službu naprosto pohřbít, jelikož by mohli preferovat platbu kartou. Otázkou je, zda by to bylo pro ně výhodné.

2.5.2. Práva a povinnosti poskytovatele nepřímého dání platebního příkazu

Poskytovatelem nepřímého dání platebního příkazu může být banka[133], družstevní záložny[134], jelikož poskytují platební služby, pod kterou spadá i nepřímé dání platebního příkazu dle ustanovení § 3, odst. 1, písm. g) ZoPS. Dalšími mohou být platební instituce[135] a instituce elektronických peněz[136].

V rámci služby nepřímého dání platebního příkazu poskytovatel:

„a) nepřijímá peněžní prostředky k provedení platební transakce,

b) zpřístupní osobní bezpečnostní prvky plátce pouze plátci a tomu, kdo je vydal,

c) sdílí údaje o plátci, s výjimkou osobních bezpečnostních prvků plátce, pouze s příjemcem a na základě výslovného souhlasu plátce,

d) neuchovává citlivé údaje o platbách plátce,

e) při každém nepřímém dání platebního příkazu osvědčí poskytovateli, který uživateli vede platební účet přístupný prostřednictvím internetu, svoji totožnost,

f) v souvislosti se službou nepřímého dání platebního příkazu nepožaduje od plátce jiné údaje o plátci než údaje potřebné k nepřímému dání platebního příkazu ani takové údaje neuchovává a nezpracovává a

---

[132] NÝDRLE, Tomáš. § 161 [*Povinnosti poskytovatele, který vede platební účet*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[133] § 1, odst. 3, písm. c) zákona 21/1992 Sb., o bankách

[134] § 3, odst. 1, písm. b) zákona 87/1995 Sb., o spořitelnách a úvěrních družstvech a některých opatřeních s tím souvisejících a o doplnění zákona České národní rady č. 586/1992 Sb., o daních z příjmů

[135] § 9, odst. 1, písm. d) zákona č. 370/2017 Sb., o platebním styku

[136] § 68, odst. 1, písm. d) Ibid.

g) nemění údaje uvedené v nepřímo daném platebním příkazu.“[137]

Písm. a) je logické, jelikož samotný princip nepřímého dání platebního příkazu spočívá v zprostředkování příkazu plátce k poskytovateli, který vede jeho platební účet a není žádný důvod, aby poskytovatel služby nepřímého dání platebního příkazu přijímal peněžní prostředky k provedení platební transakce. S tím je spojené i písm. g), kdy poskytovatel nepřímé dání platebního příkazu nesmí měnit údaje v platebním příkazu, jelikož z povahy služby má pouze tyto informace předat poskytovateli, který vede platební účet plátce a je vázán vůlí plátce.

Osobním bezpečnostním prvkem uvedeným v písm. b) se rozumí „prvek, který poskytovatel poskytl uživateli za účelem ověření“.[138]

Poskytovatel může sdílet údaje o plátci pouze příjemci s výslovným souhlasem plátce a žádným dalším osobám. Tento výslovný souhlas stačí, aby byl uveden ve smlouvě o platebních službách.[139]

Dále poskytovatel „neuchovává citlivé údaje o platbách plátce“[140].Citlivým údajem o platbách uživatele se rozumí „údaj, který může být zneužit k podvodu v oblasti platebních služeb, s výjimkou jedinečného identifikátoru a jména majitele platebního účtu v případě poskytovatele služby informování o platebním účtu nebo služby nepřímého dání platebního příkazu“.[141]

O písm. e) jsem se už v kapitole 2.5.1. zmínil, že k osvědčení poskytovatelů, který vede platební účet, se „využívají kvalifikované certifikáty pro elektronické pečetě (srov. čl. 3 bodu 30 nařízení eIDAS) nebo kvalifikované certifikáty pro autentizaci internetových stránek (srov. čl. 3 bodu 39 nařízení eIDAS)“[142].

Vzhledem k tomu, že předání platebního příkazu od poskytovatele služby nepřímého dání platebního příkazu by mělo probíhat přes API rozhraní, které vytvoří poskytovatel, který vede platební účet nebo prostřednictvím screen scraping, musí poskytovatel služby nepřímého dání platebního příkazu získat určité vstupní údaje od plátce, aby mohl tento příkaz předat. Může jít o přihlašovací údaje,

---

[137] § 162 zákona č. 370/2017 Sb., o platebním styku

[138] § 2, odst. 3, písm. m) zákona č. 370/2017 Sb., o platebním styku

[139] NÝDRLE, Tomáš. § 162 [*Povinnosti poskytovatele nepřímého dání platebního příkazu*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[140] § 162 písm. d) zákona č. 370/2017 Sb., o platebním styku

[141] § 2, odst. 3, písm. n) zákona č. 370/2017 Sb., o platebním styku

[142] NÝDRLE, Tomáš. § 162 [*Povinnosti poskytovatele nepřímého dání platebního příkazu*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

aby mohl poskytovatel předat platební příkaz přes jeho uživatelské rozhraní. Tyto údaje nemá dále uchovávat ani zpracovávat.[143]

2.6. Využití v praxi

Výše uvedené novinky, jmenovitě služba informování o platebním účtu a služba nepřímé dání platebního příkazu, dle mého názoru jsou právě služby, které jsou zásadní pro prosazení nové technické vlny v bankovnictví. Tyto služby propojují třetí strany se službami a usnadňují uživateli třeba mít na jednom místě všechny platební účty, které má otevřené u bank a další služby, které mohou být v budoucnu dostupné uživateli. Navíc dává obchodníkům možnost, jak se odklonit od spolupráce s karetními asociacemi při platbě od zákazníka, což bych jako obchodník velmi kvitoval, zejména kvůli poplatkům, které obchodníci musí zaplatit za každou platbu karetní asociaci.

Studie společnosti Deloitte z roku 2018 tvrdí, že uživatelé v České republice jsou konzervativními klienty, jelikož pouze 18 % uživatelů by sdílelo informace o svém platebním účtu za účelem lepších služeb s některou z jiných bank, což v jiných východoevropských zemích činilo až 35 % uživatelů, kteří by byli ochotní za lepší služby poskytnout tato data. Motivovat by je mohly lepší nabídky úvěru nebo kreditní skóre (viz kapitola 2.6.3.).[144]

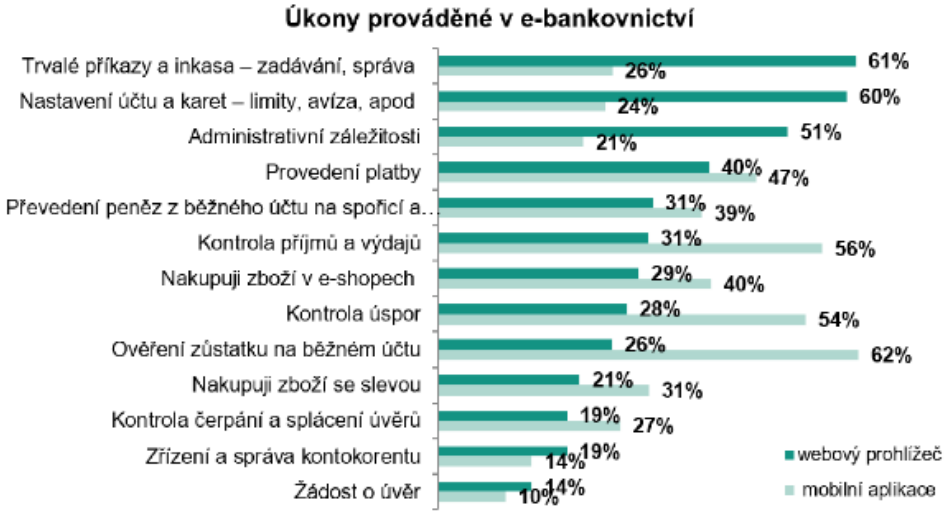
Průzkum Češi a digitalizace 2020, kterou provedla České bankovní asociace ukázal, že 97 % klientů bank používá internetové bankovnictví, což je 15 % nárůst oproti roku 2018.[145] Obrovský nárůst uživatelů si vysvětluji zejména pandemií koronaviru COVID-19, který znemožnil lidem chodit běžně vyřizovat na pobočku standardní záležitosti.

[143] NÝDRLE, Tomáš. § 162 [*Povinnosti poskytovatele nepřímého dání platebního příkazu*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[144] Studie Deloitte: České banky i uživatelé jsou na PSD2 v regionu nejlépe připraveni. *Deloitte Česká republika* [online]. [cit. 2021-03-15]. Dostupné z:

[145] Češi a digitalizace 2020. *Česká bankovní asociace* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/cesi-a-digitalizace-2020

Obrázek 2 *– Úkony prováděné v e-bankovnictví*



Upraveno ze zdroje: Češi a digitalizace 2020. *Česká bankovní asociace* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/cesi-a-digitalizace-2020

Obrázek 2 ukazuje úkony, které provádí klienti v internetovém bankovnictví. Na obrázku 2 je vidět, ke kterým činnostem klienti používají internetový prohlížeč a ke kterým mobilní aplikaci, avšak to není dle mého názoru v této kapitole důležité. Důležité je to, že vidíme určitý rozptyl služeb, které využívají klienti a z toho můžeme vyvodit, zda jsou spíše konzervativními uživateli, jak zmiňuje výše studie společnosti Deloitte nebo používají i jiné služby, které jim může nabídnout směrnice PSD2 či služby nad rámec směrnice PSD2 či samotného ZoPS.

Myslím si, že žádost o úvěr, nákup zboží se slevou nebo nákup zboží v e-shopech může být ukazatel toho, že by tito lidé mohli v budoucnu využít scoring nebo nepřímé dání platebního příkazu. Z výzkumu od České bankovní asociace také vyplývá, že jde hlavně o strach z nedostatku bezpečnosti, který brzdí využití nových služeb. Pokud poskytovatelé platebních služeb a třetí strany se budou snažit v této oblasti zapracovat na veřejném mínění, může jim to do budoucna prospět na českém trhu a získat více klientů.

2.6.1. Multibanking

Jedním z produktů spojení služeb informace o platebním účtu, nepřímé dání platebního příkazu a potvrzování zůstatku peněžních prostředků pro vydavatele karetních prostředků, které jsou nově dostupných ze směrnice PSD2, jsou multibanking aplikace. Multibanking aplikace umožňuje uživatelům připojit do

aplikace všechny bankovní účty, se kterými disponují a mají přístup pouze z jedné aplikace, kde nepostrádají základní funkcionalitu.

První českou multibanking aplikací byla Richee a to už v červenci 2018, kterou spustila Banka CREDITAS.[146] Současný stav je takový, že každá aplikace má omezený počet bank, ke které se může uživatel připojit. V tomto je nejdále Banka Creditas, která umožňuje připojení z 14 bank, například J&T Banka, Moneta Money Bank. Některé banky, které sdílí data, nenabízejí vůbec multibanking. Jde například o Fio banku, Raiffeisen Bank nebo rovněž Equa bank.[147]

Otázkou je, jak moc je multibanking využívanou službou napříč uživateli. Z průzkumu Češi a digitalizace 2019 od České bankovní asociace vyplývá, že 47 % dotázaných ve výzkumu uvedlo, že považují multibanking za přínosný ve složení 15 % určitě ano a 47 % spíše ano, což není dle mého názoru moc lichotivý výsledek.[148] Může to být i tím, že mnoho uživatelů nemá více účtů a používá pouze jeden. Já osobně používám dva bankovní účty od dvou bank a nemám stále potřebu si propojit jednu či druhou aplikaci s účtem od jiné banky. Zaprvé je to otázka bezpečnosti, o kterou se bojí i další uživatelé, což ve výzkumu od České bankovní asociace potvrdilo 23 % respondentů[149] a zadruhé je to pro mě řešení na půl cesty. Pokud si chci objednat novou platební kartu, dejme tomu k účtu u České spořitelny, na aplikaci od Komerční banky takovou operaci neuskutečním. Nedělám to každý den, ale chci mít tu možnost a raději budu mít dvě aplikace na mobilu než jednu.

Nemilou zprávou je to, že 8 % dotázaných se vyjádřilo, že používají multibanking a 8 % respondentů přijde složité manipulovat s multibanking funkcí, a to může být námětem pro banky k tomu, aby zapracovaly na svých aplikacích s mobilním bankovnictví celkově.[150]

2.6.2. Správa financí

Aplikací na správu financí je na trhu nespočet, avšak mezi ty nejvíce doporučované se řadí aplikace z českých společností, jmenovitě Spendee, která vyvíjí stejnojmennou aplikaci a BudgetBakers aplikaci Wallet. O těchto

[146] První česká multibankovní aplikace Richee. Pro CREDITAS ji vytvořila česká IT společnost Cleverlance. *Cleverlance* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://www.cleverlance.de/cz/novinky/Stranky/Richee.aspx

[147] Multibanking 2021: Jak funguje a které banky ho podporují? *Skrblík.cz* [online]. [cit. 2021-03-15]. Dostupné z: https://www.skrblik.cz/finance/ucty/multibanking/

[148] Češi a digitalizace 2019. *Česká bankovní asociace* [online]. 2019 [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/cesi-a-digitalizace-2019

[149] Ibid.

[150] Ibid.

společnostech jsem se už zmínil na začátku kapitoly a není třeba si je více představovat. Aplikace správy financí mají pomáhat uživatelům k tomu, aby měli pod dohledem své měsíční výdaje a příjmy.

Konkrétně tyto dva startupy mají povolení k činnosti jako správce informací o platebním účtu, což znamená, že můžou stahovat data z bankovních účtů uživatelů, kteří k nim mají přístup. Přes API rozhraní se stáhnou data o příjmech a výdajích, které potom zpracovává aplikace a uživatel si může například nechat spočítat, za které položky utratil v měsíci nejvíc nebo kolik utrácí za předplatné. Nutno dodat, že stahování dat z účtu je u obou aplikací dostupné v předplaceném programu.

Z vlastní zkušeností vím, že zapisování dat do peněženky z každé útraty bylo velmi nekomfortní. Aplikaci jsem navíc příliš nevyužíval i proto, že jsem necítil potřebu platit za to, aby mi aplikace stahovala data z mých bankovních účtů.

2.6.3. Scoring

Scoring je pojem, se kterým se setkáváme zejména v souvislosti s poskytováním úvěrů nebo hypotečních úvěrů. Banka žadatele o úvěr na základě scoringu ověří jeho bonitu, zda splňuje požadavky úvěruschopnosti k tomu, aby mohl daný úvěr získat a zvládat splácet.[151] Ostatně na stránkách Finančního arbitra můžeme narazit na nespočet rozhodnutí arbitra o špatném posouzení úvěruschopnosti žadatele ze strany banky nebo nebankovních poskytovatelů. Dle mého názoru může správné posouzení bonity prostřednictvím využití služby informování o platebním účtu velmi lehce tento problém vyřešit, pokud bude vůle bank a obzvlášť nebankovních poskytovatelů.

V České republice získal povolení k činnosti v roce 2020 zatím poslední správce informací o platebním účtu, a to společnost 1. PF Finance, která se zaměřuje právě na scoring, poskytuje tyto služby pro kreditní a leasingové společnosti. Nabízí „soubor významných transakcí, jméno vlastníka účtu, seznam stálých plateb (plateb), maximální příchozí a odchozí platby.“[152]

[151] Scoring u hypotéky. *Banky.cz* [online]. [cit. 2021-03-16]. Dostupné z: https://www.banky.cz/hypotecni-slovnik/scoring-u-hypoteky/

[152] *1. PF Finance, s.r.o.* [online]. [cit. 2021-03-16]. Dostupné z: https://www.1pffin.cz/

3. Silné ověření uživatele

Silné ověření uživatele považuji za jednu z klíčových úprav, které přinesla směrnice PSD2, kterou členské státy Evropské Unie musely implementovat do svých vnitrostátních právních řádů.

Silné ověření uživatele by mělo chránit uživatele před neautorizovanou platbou a snížit riziko podvodů. Zákonodárce důvod bezpečnosti placení přes internet zdůrazňuje i v důvodové zprávě. Zdůrazňuje, že změna oproti stavu před ZoPS je zákonná povinnost, jelikož do doby účinnosti ZoPS probíhalo silné ověření uživatele na dobrovolné bázi na základě doporučení Evropského orgánu pro bankovnictví.[153] Otázkou je, zda technologický vývoj a dané technické parametry dané směrnicí PSD2, potažmo nařízení RTS týkající se silného ověření uživatele, budou časem stále dostatečné.

Ustanovení článku 98 směrnice PSD2 určuje, aby regulační technické normy týkající se ověřování a komunikace vypracoval Evropský orgán pro bankovnictví. Po zdlouhavém procesu bylo v listopadu 2017 vydáno v Úředním věstníku Evropské unie nařízení RTS, které vstoupilo v platnost v březnu 2019. Avšak obavy z nereflektování technologického vývoje rozbíjí odstavec 5 článku 98 PSD2: „EBA v souladu s článkem 10 nařízení (EU) č. 1093/2010 regulační technické normy pravidelně přezkoumává a v případě potřeby aktualizuje s ohledem na mimo jiné inovace a technologický rozvoj.“[154] Regulační technické normy „jsou technické povahy a nepředstavují strategická či politická rozhodnutí a jejich obsah je vymezen legislativními akty, z nichž vycházejí.“[155] Regulační technické normy zpracoval Evropský orgán pro bankovnictví, který má pravomoc vydávat dále obecné pokyny a doporučení na základě nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro bankovnictví).

Směrnice PSD ani v ZoPS z 2009 nezahrnovaly technické otázky k zabezpečení při autorizaci platební transakce. Doplňovaly je obecné pokyny od Evropského orgánu pro bankovnictví k bezpečnosti internetových plateb

[153] Důvodová zpráva k zákonu č. 370/2017 Sb. o platebním styku, č. 370/2017 Dz

[154] Článek 98, odst. 5 směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES

[155] Článek 10 nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro bankovnictví), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/78/ES

EBA/GL/2014/12[156]. Nutno dodat, že obecné pokyny a doporučení od Evropského orgánu pro bankovnictví ovlivňují interpretaci všech úprav v ZoPS a dalších právních úprav v rámci bankovnictví, jak je známo z praxe. V běžné praxi se zachází se mi všemi doporučení od Evropského orgánu pro bankovnictví a banky jako s obecnými pokyny.

Silné ověření uživatele, někdy se setkáváme s jinými termíny jako silné ověření klienta (terminologie ze směrnice PSD2), v odborných článcích a literatuře pod anglickým termínem Strong Customer Authorization nebo zkratkou SCA. Silné ověření uživatele "je bezpečnostní mechanismus, který si klade za cíl zásadním způsobem snížit riziko vzniku podvodů v důsledku kompromitovaného (uniklého, nebo zneužitého) hesla"[157]. Využívá k tomu kombinaci 2 ze tří prvků, které jsou dané zákonem. Tyto prvky rozeberu později v kapitole 3.1.

Ustanovení článku 97 směrnice PSD2 udává, že silné ověření uživatele se použije v případě, pokud uživatel:

„a) využívá on-line přístupu ke svému platebnímu účtu;

b) iniciuje elektronickou platební transakci;

c) prostřednictvím prostředků komunikace na dálku provede jakýkoli úkon, který by mohl vést k riziku platebního podvodu nebo jiných zneužití."[158]

Dále článek 97 směrnice PSD2 uvádí: „Pokud jde o iniciaci elektronické platební transakce uvedenou v odst. 1 písm. b) členské státy zajistí, aby u elektronických platebních transakcí na dálku poskytovatelé platebních služeb uplatňovali silné ověření klienta, jež zahrnuje prvky dynamicky propojující transakci s konkrétní částkou a konkrétním příjemcem."[159]

Český zákonodárce implementoval ustanovení článku 97 směrnice PSD2 do poněkud jiné formy, která se nijak v zásadě neliší od původní myšlenky, ale přizpůsobuje se české terminologii v ZoPS:

„a) přistupuje ke svému platebnímu účtu prostřednictvím internetu,

---

[156] NÝDRLE, Tomáš. § 223 [Vymezení a použití silného ověření uživatele]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. Wolters Kluwer [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[157] EISELT, Zbyněk. Co znamená silné ověření klienta (SCA) a proč se o něm všude mluví? *GoPay blog* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://www.gopay.com/blog/co-znamena-silne-overeni-klienta-sca-a-proc-se-o-nem-vsude-mluvi/

[158] Článek 97, odst. 1 směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES

[159] Článek 97, odst. 2 Ibid.

b) dává platební příkaz k elektronické platební transakci,
c) provádí jiný úkon, který je spojen s rizikem podvodu v oblasti platebního styku, zneužitím platebního prostředku nebo informací o platebním účtu, nebo
d) požaduje informace o platebním účtu prostřednictvím poskytovatele služby informování o platebním účtu."[160]

Dále v odstavci 2: „Dává-li uživatel platební příkaz prostřednictvím internetu nebo prostřednictvím elektronického zařízení, které lze použít k dálkové komunikaci, nebo dává-li platební příkaz nepřímo, osoba oprávněná poskytovat platební služby použije silné ověření uživatele, které zahrnuje jednorázové prvky propojující platební transakci s přesnou částkou a určitým příjemcem."[161]

Pokud shrnu předcházející body, které jsou dané ze zákona, znamená to vzdálený přístup a klient není přímo v kontaktu se svým poskytovatelem služeb.[162]

Znění ustanovení § 223 ZoPS se může zdát jednoznačná, ale při bližším pohledu, tomu tak zdaleka není a existuje více interpretací.

Přístup k platebnímu účtu prostřednictvím internetu není přesněji definován jak v zákoně o platebním styku, tak ani ve směrnici PSD2 a ani v nařízení RTS. Komentář k danému ustanovení hovoří ve smyslu, že se jedná: „zpřístupnění uživatelského rozhraní, které uživateli umožňuje získávat informace o platebním účtu (provedené platby, zůstatek, platební prostředky vydané k platebnímu účtu) a popřípadě následně z tohoto rozhraní dávat platební příkazy[163]". Podle mého mínění jde o klasický přístup do internetového bankovnictví. Žádné další podobné rozhraní, které popisuje přímo komentář v dnešní době neexistuje. Internetové bankovnictví může být dostupné, jak z klasického webového prohlížeče, tak i z mobilní aplikace.

Při dání platebního příkazu je také povinné silné ověření uživatele. Za takový platební příkaz lze považovat každý platební příkaz, který je dán

[160] § 223, odst. 1 zákona č. 370/2017 Sb., o platebním styku
[161] § 223, odst. 2 Ibid.
[162] Důvodová zpráva k zákonu č. 370/2017 Sb. o platebním styku, č. 370/2017 Dz
[163] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

elektronickými prostředky (například internetové, mobilní bankovnictví, platbomat nebo platební kartou)[164] [165].

Úkon s rizikem podvodu v oblasti platebního styku, který zákonodárce implementoval do písmene c), výslovně neurčuje, že jde o úkony na dálku, avšak dle důvodové zprávy se tak dá dovodit, jak jsem zmiňoval výše. Výklad těchto úkonů není zcela jasný, ale komentář k ZoPS se zmiňuje například o zjištění zůstatku účtu prostřednictvím bankomatu[166].

Jedním z posledních jsou informace o platebním účtu prostřednictvím poskytovatele služby informování o platebním účtu (viz kapitola 2.4).

V případě, že uživatel zadává platební transakci propojující přesnou částku s určitým příjemcem přes elektronické zařízení nebo prostřednictvím internetu, je rovněž potřeba využít silného ověření uživatele. ZoPS doplňuje oproti směrnici PSD2 povinnost o nepřímé dání platebního příkazu[167], kterému se věnuji v kapitole 2.4.

Od 1. ledna 2021 musí všichni poskytovatelé platebních služeb při placení platební kartou využít silného ověření uživatele. Tato povinnost platí i pro „další subjekty podílející se na zpracování platební transakce (vč. obchodníků a provozovatelů platebních bran, provozovatelů karetních schémat atd.)“[168]

3.1. Prvky ověření

Pojem ověření je definován v ustanovení § 2 odst. 3, písm. l) ZoPS, které znamená „ověřením postup umožňující poskytovateli ověřit totožnost uživatele nebo oprávněné použití platebního prostředku nebo osobních bezpečnostních prvků uživatele[169]“.

---

[164] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[165] SOUKAL, Marek. Silné ověření klienta při poskytování platebních služeb. Epravo.cz [online]. 2019 [cit. 2021-02-23]. Dostupné z: https://www.epravo.cz/top/clanky/silne-overeni-klienta-pri-poskytovani-platebnich-sluzeb-109952.html

[166] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[167] Ibid.

[168] Silné ověření uživatele u plateb kartou na internetu od 1. 1. 2021. Česká národní banka [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/vykon-dohledu/upozorneni-pro-verejnost/Silne-overeni-uzivatele-u-plateb-kartou-na-internetu-od-1.-1.-2021/

[169] § 2, odst. 3, písm. l) zákona č. 370/2017 Sb., o platebním styku

V nařízení RTS můžeme najít následující prvky: znalost (*anglicky:* knowledge), držení (*anglicky:* possession) a inherence (*anglicky:* inherence).[170] Silné ověření uživatele se provádí při ověření ze dvou, ze tří dostupných prvků, jejichž výčet je taxativně uveden v ustanovení § 223, odst. 3 ZoPS:

„a) údaje, který je znám pouze uživateli,

b) věci, kterou má uživatel ve své moci,

c) biometrických údajů uživatele.“[171]

Bližší specifikace těchto prvků je obsažena v nařízení RTS a ve stanovisku Evropského orgánu pro bankovnictví pod označením EBA-Op-2019-06.

V první řadě je třeba zmínit, že tyto prvky „musí být vzájemně nezávislé a prolomení jednoho prvku nesmí ovlivnit spolehlivost prvků ostatních“ [172] s následujícími kritérii:

„a) použití odděleného bezpečného prostředí pro provedení prostřednictvím softwaru nainstalovaného ve víceúčelovém zařízení;

b) mechanismy k zajištění toho, aby software nebo zařízení nebyly pozměněny plátcem nebo třetí stranou;

c) došlo-li ke změnám, mechanismy k zmírnění jejich důsledků.“[173]

3.1.1 Znalost

„Údaje, který je znám pouze uživateli“[174], takto neurčitě je určen prvek znalosti v ZoPS. ZoPS jej nijak dále nevymezuje. Směrnice PSD2 se zmiňuje o tom, že prvek znalosti je „to, co ví pouze uživatel“[175]. Výklad ustanovení § 223, odst. 3, písm. a) ZoPS musíme opřít o stanovisko EBA-Op-2019-06, které vydal Evropský orgán pro bankovnictví v polovině 2019, jelikož nařízení RTS podobně jako ZoPS v článku 6 neobjasňuje o moc víc.

---

[170] Článek 4, odst. 1 nařízení Komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace

[171] § 223, odst. 3 zákona č. 370/2017 Sb., o platebním styku

[172] § 223, odst. 4 Ibid.

[173] Článek 9, odst. 3 nařízení Komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace

[174] § 223, odst. 3, písm. a) zákona č. 370/2017 Sb., o platebním styku

[175] Článek 4, odst. 30 Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES

Nutno dodat, že stanovisko Evropského orgánu pro bankovnictví nenabízí taxativní výčet elementů, které se dají považovat za prvek znalosti a v budoucnosti může být upraven dalším stanoviskem.

Za prvek znalosti se v současné době považuje zejména:

a) heslo[176],

b) PIN[177],

c) otázky založené na předchozí znalosti[178],

d) heslová fráze[179], a

e) memorised swiping path (volně přeloženo jako znak na obrazovce mobilního telefonu[180] nebo zamykací gesto)[181].

Stanovisko Evropského orgánu pro bankovnictví za prvek znalosti nepovažuje:

a) uživatelské jméno[182],

b) e-mailová adresa[183],

c) údaje na platební kartě (například číslo platební karty, CVV/CVC kód, platnost karty)[184],

d) jednorázové heslo generované nebo přijaté na zařízení (například na mobilním telefonu)[185], a

e) TAN listy (papírové seznamy jednorázových autentizačních kódů)[186].

---

[176] Bod 32, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019, s. 8.

[177] Ibid.

[178] Ibid.

[179] Ibid.

[180] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[181] Bod 32, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019, s. 8.

[182] Bod 34, Ibid.

[183] Ibid.

[184] Bod 33, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019, s.8.

[185] Bod 35, Ibid.

[186] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

Neméně důležitý je výklad toho, co znamená pojem „znám pouze uživateli[187]“. Nařízení RTS se zmiňuje o tom, že „poskytovatelé platebních služeb přijmou opatření k zmírnění rizika toho, že prvky silného ověření klienta z kategorie znalosti jsou použity neoprávněnými stranami.“[188] Z toho se dá vyvodit, že pokud dodrží poskytovatel platebních služeb všechna opatření k tomu, aby se k těmto údajům nedostala neoprávněná osoba, nebude poskytovatel platebních služeb odpovědný za to, pokud prvek znalosti nějakým způsobem uživatel například „jednáním, opomenutím či nedostatečného zabezpečení“[189] poskytne neoprávněné osobě tyto údaje. Nutno také dodat, že při vyzrazení prvku znalosti jej nelze v budoucnosti nadále používat.[190]

Pro srovnání, v minulosti podle obecných pokynů od Evropského orgánu pro bankovnictví k bezpečnosti internetových plateb EBA/GL/2014/12, údaje na platební kartě, například CVV/CVC kód byl akceptován jako prvek znalosti. Podle novějšího stanoviska EBA-Op-2019-06 už podle současné úpravy nikoliv.[191] Dle mého názoru je to správný krok, byť je to pro některé méně komfortní krok, na který si mnozí už postupem času zvykli.

3.1.2. Držení

ZoPS definuje prvek držení jako “věci, kterou má uživatel ve své moci”[192]. Na pomoc můžeme k výkladu použít definici věci, která znamená „vše, co je rozdílné od osoby a slouží potřebě lidí“[193]. Směrnice PSD2 popisuje, že držení je „to, co drží pouze uživatel“[194]. Stanovisko EBA-Op-2019-06, které vydal Evropský

[187] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[188] Článek 6, odst. 1 nařízení Komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace

[189] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[190] Ibid.

[191] Bod 33, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019, s.8.

[192] § 223, odst. 3, písm. b) zákona č. 370/2017 Sb., o platebním styku

[193] § 489 zákona č. 89/2012 Sb, občanský zákoník

[194] Článek 4, odst. 30 směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES

orgán pro bankovnictví doplňuje, že nejde pouze o hmotnou věc, nýbrž může jít i o věci nehmotné, například mobilní aplikace.[195] ZoPS se dále podrobněji nezmiňuje o prvku držení, avšak opět ani nařízení RTS, konkrétně v článku 7 nebyl evropský zákonodárce o moc více konkrétní, a tedy neposkytl více podrobností. Poskytovatel platebních služeb má i v prvku držení přijmout opatření k zmírnění rizika použití neoprávněnými osobami.[196] Prvek držení by ve své moci měl mít tedy pouze uživatel a žádná další osoba. Uživatel by měl být natolik odpovědný a i zde „svým jednáním, opomenutím“[197] by neměl umožnit přístup k tomuto prvku další osobě. Z nařízení RTS uživateli přímo vyplývá povinnost opatření k zabránění replikace prvků držení. Odlišnost od prvku znalosti spočívá v tom, že v případě dočasného se zmocnění prvku neoprávněnou osobou a následným navrácením uživateli lze prvek nadále používat k ověření.[198]

Stanovisko EBA-Op-2018-04 Evropského orgánu pro bankovnictví určuje, že k tomu, aby zařízení mohlo být použito jako prvek držení „musí existovat spolehlivý prostředek k potvrzení držení prostřednictvím vygenerování nebo přijetí prvku dynamického ověření na zařízení“[199]. Takovým prostředkem pro potvrzení může být jednorázový kód, vygenerovaný softwarem, hardwarem jako token, textová zpráva nebo notifikace.[200] Nutno dodat, že samotná textová zpráva není prvkem držení, ale SIM karta, která je spojená s telefonním číslem jím je.[201] Generování jednorázového kódu na zařízení může být provedeno přes aplikaci Google Authenticator[202] nebo Microsoft Authenticator, který mi přijde osobně za velmi intuitivní a nutný základ pro přihlašování k internetovým účtům v dnešní

[195] Bod 24, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019, s.6.

[196] Článek 7, odst. 1 nařízení Komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace

[197] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[198] Ibid.

[199] Bod 35, European Banking Authority. EBA-Op-2018-04: Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC ze dne 13. června 2018, s.7.

[200] Bod. 25, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 z 21. června 2019, s.6.

[201] Ibid.

[202] SOUKAL, Marek. Silné ověření klienta při poskytování platebních služeb. *Epravo.cz* [online]. 2019 [cit. 2021-02-23]. Dostupné z: https://www.epravo.cz/top/clanky/silne-overeni-klienta-pri-poskytovani-platebnich-sluzeb-109952.html

době, kdy se kybernetická bezpečnost se stále velice zlehčuje a přístup k našim internetovým účtům nemáme tak zabezpečený, jak bychom mohli a měli mít.

Za zajímavou považuji skutečnost, že prvek držení může být založen například na aplikaci, který by měl být provázán se zařízením a uchováván přes šifrování v bezpečnostním čipu.[203]

Stanovisko EBA-Op-2019-06 Evropského orgánu pro bankovnictví ani v tomto případě není taxativní. Za prvky držení považuje, zejména:

a) zařízení potvrzené jednorázovým kódem, generovaný nebo přijatý na zařízení (hardware nebo softwarový token generátor, textová zpráva s jednorázovým kódem[204],

b) zařízení potvrzený podpisem generovaným zařízením (hardware nebo softwarový token)[205],

c) karta nebo zařízení potvrzený přes QR kód (nebo fotografií TAN listu) skenovaný externím zařízením[206], a

d) mobilní aplikace nebo webový prohlížeč, jehož držení je navázán na zařízení – například přes bezpečnostní čip v zařízení nebo privátní klíč, který propojuje aplikaci k zařízení nebo propojení webového prohlížeče k zařízení[207].

Za prvek držení se nedá považovat údaje na platební kartě[208] (například CVC/CVV kód), který se nepokládá ani za prvek znalosti (viz kapitola 3.1.1).

3.1.3. Inherence

Inherencí se rozumí ověření pomocí „biometrických údajů uživatele[209]“. Tento široký pojem se ve směrnici PSD2 definuje jako „to, čím uživatel je[210]“.

Troufám si tvrdit, že prvek inherence bude jedním z preferovanějších prvků, které si uživatel zvolí, jelikož díky technologickému pokroku máme valná většina chytré telefony, které dokážou naše biometrické údaje zaznamenat. Alespoň já osobně prvek inherence využívám nejvíce při silném ověření uživatele v kombinaci

[203] Bod. 26, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019 ,s.6.

[204] Table 2, Ibid.

[205] Ibid.

[206] Ibid.

[207] Ibid.

[208] Ibid.

[209] § 223, odst. 3, písm. c) zákona č. 370/2017 Sb., o platebním styku

[210] Článek 4, odst. 30 směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES

s prvkem znalosti. Podle odhadů z roku 2018, mohlo proběhnout v roce 2020 až 126 mld. transakcí v hodnotě kolem 1,1 bilionů USD.[211]

Otázkou je, co znamenají biometrické údaje uživatele. Komentář k ZoPS zmiňuje: „Biometrie je vymezena jako biologický vědní obor zabývající se zjišťováním kvantitativních znaků (délky, výšky apod.) organismů (Havránek a kol., 1989, k heslu biometrie). Biometrický údaj lze tedy vymezit jako měřitelný fyzický znak uživatele. Nařízení GDPR vymezuje biometrické údaje jako osobní údaje vyplývající z konkrétního technického zpracování týkajícího se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje“[212].

Další zdroj se zmiňuje o tom, že: „Biometrikami rozumíme jedinečné, měřitelné, anatomické, fyziologické nebo behaviorální charakteristiky člověka, přičemž v praxi využíváme ty biometriky, které jsou stálé a které je možné bez nepřiměřených obtíží automatizovaně změřit a naměřená data dále zpracovávat, jako např. otisk prstu, vzor oční duhovky či sítnice, geometrie ruky, charakteristiky tváře či hlasu“[213].

Z toho můžeme dovodit, že tyto údaje jsou anatomicky a fyziologicky dané, jedinečné nebo ze znaků chování daného uživatele. Je potřeba zdůraznit, že nařízení RTS ukládá povinnost poskytovateli platebních služeb zmírnit riziko, aby nebyly zneužity neoprávněnou osobou, zejména u zařízení a softwaru.[214]

Stanovisko EBA-Op-2019-06 Evropského orgánu pro bankovnictví uvádí
a) následující příklady toho, co se dá považovat za prvky inherence:
b) sken otisku prstů[215],

---

[211] TOMÍŠEK, Jan. Právní jednání biometrickými prostředky v elektronickém bankovnictví. *Právní rozhledy*, 2018, č. 5, s. 160-167

[212] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[213] TOMÍŠEK, Jan. Právní jednání biometrickými prostředky v elektronickém bankovnictví. *Právní rozhledy*, 2018, č. 5, s. 160-167

[214] Článek 8, odst. 1 nařízení Komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace

[215] Bod. 19, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019, s. 5.

c) rozpoznání hlasu[216],

d) rozpoznání žil[217],

e) geometrie ruky a obličeje k identifikaci uživatelova obličeje či ruky[218],

f) skenování sítnice a duhovky[219],

g) dynamika stisknutí kláves[220],

h) srdeční frekvence nebo jiné vzorce pohybu těla[221] (u nositelných zařízení, například Apple Watch), a

i) úhel ve kterém je zařízení držen[222].

Mezi prvky inherence StanoviskoEBA-Op-2019-06 nepokládá memorised swiping path (volně přeloženo jako znak na obrazovce mobilního telefonu nebo zamykací gesto)[223] nebo informace přenášené pomocí komunikačního protokolu, jako například EMV® 3-D Secure[224].

Nejprve je potřeba jeden z těchto prvků zaregistrovat v daném zařízení[225]. Typickým příkladem je mobilní telefon, přičemž já osobně používám Apple iPhone se zabudovanou technologii FaceID, která rozpoznává obličej uživatele pomocí vyvinuté technologie společností Apple. Tato informace se uloží v šifrovaném úložišti/čipu (záleží na modelu daného telefonu) po registraci tohoto prvku v zařízení. Můžeme zde jen polemizovat o tom, zda je bezpečné svěřit své jedinečné údaje (například oční rohovka a otisk prstu) výrobci, byť s dobrým compliance na uchovávání osobních dat. Obzvlášť v současné době, kdy takřka každý rok se dostane na veřejnost zpráva, ve kterém oznamuje velký únik osobních dat. Například ten, který se „povedl" americkému Facebooku[226] v roce 2019 nebo

---

[216] Bod. 19, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019, s. 5.

[217] Ibid.

[218] Ibid.

[219] Ibid.

[220] Ibid.

[221] Ibid.

[222] Table 1, European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019, s. 35

[223] Bod 20, Ibid., s. 5.

[224] Bod 21, Ibid., s. 5.

[225] TOMÍŠEK, Jan. Právní jednání biometrickými prostředky v elektronickém bankovnictví. *Právní rozhledy*, 2018, č. 5, s. 160-167

[226] Facebook přiznal obří únik dat. Útočníci se dostali k 50 milionům uživatelských účtů. *INFO.CZ* [online]. 2018 [cit. 2021-02-22]. Dostupné z: https://www.info.cz/zpravodajstvi/svet/facebook-priznal-obri-unik-dat-utocnici-se-dostali-k-50-milionum-uzivatelskych-uctu

britskému BioStar 2[227] v roce 2018, kdy unikly přímo otisky prstů a kontury obličeje. O to horší, že v případě BioStar 2 jej používaly britské banky i metropolitní policie. Ruku v ruce s tím jde také riziko přístupu dalších osob do mobilního telefonu, nýbrž i možného obejití silného ověření uživatele, které mají rovněž nastavený přístup, kromě samotného uživatele. Ze své vlastní zkušenosti vím, že kvůli pohodlí mám přístup přes TouchID (technologie snímající otisky prstů) do mobilního telefonu svých rodičů, kteří jej však nepoužívají k přístupu do internetového bankovnictví ze svého přesvědčení.

V tomto případě nemá banka nad těmito prvky žádnou kontrolu a musí důvěřovat třetí straně. Přínosem je, že neručí za ztrátu těchto dat.[228]

3.1.4. Mobilní aplikace „klíč“

Poslední rok a půl zaznamenávám, že banky hledají nové cesty a v praxi už nabízejí nové způsoby, jak dostát požadavku splnění 2 ze 3 prvků při silném ověření uživatele. Je to komfortní v případě, že vlastníte chytrý telefon, který má alespoň snímač otisku prstů (například TouchID od Apple) nebo rozpoznání obličeje (například FaceID od Apple).

Tyto mobilní aplikace se většinou nazývají klíč, například George klíč od České spořitelny nebo KB klíč od Komerční banky. Tyto „klíče“ v sobě kombinují 3 prvky[229]:

a) prvek držení – zařízení,

b) prvek znalosti – PIN, který si nastaví uživatel v aplikaci, a

c) prvek inherence – otisk prstu či rozpoznání obličeje.

Platí zde to, že „musí existovat spolehlivý prostředek k potvrzení držení prostřednictvím vygenerování nebo přijetí prvku dynamického ověření na zařízení“[230], jinak by v tomto případě prvek držení nemohl být uznán.

---

[227] Otisky prstů i osobní údaje. Bezpečnostní firma nechala na internetu 23 gigabytů nechráněných dat. *IROZHLAS* [online]. [cit. 2021-02-22]. Dostupné z: https://www.irozhlas.cz/veda-technologie/hash-otisky-prstu-rozpoznani-obliceje-unik-dat-databaze-guardian-kauza-vedci_1908160800_mpr

[228] TOMÍŠEK, Jan. Právní jednání biometrickými prostředky v elektronickém bankovnictví. *Právní rozhledy*, 2018, č. 5, s. 160-167

[229] Česká spořitelna spouští aplikaci George klíč pro všechny klienty. *Česká spořitelna* [online]. 2019 [cit. 2021-02-23]. Dostupné z: https://www.csas.cz/cs/o-nas/pro-media/tiskove-zpravy/2019/09/11/ceska-sporitelna-spousti-aplikaci-george-klic-pro-vsechny-klienty

[230] Bod 35, European Banking Authority. EBA-Op-2018-04: Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC ze dne 13. června 2018, s.7.

3.2. Výjimky ze silného ověření klienta

Nařízení RTS udává výjimky, kdy poskytovatel platební služby nemusí provést silné ověření klienta.

3.2.1. Informování o platebním účtu

V článku 10 nařízení RTS je stanovena výjimka, kdy se neužije silné ověření uživatele v případě informování o platebním účtu, kdy třetí strana získá přístup k zůstatku na platebním účtu a k platebním transakcím v posledních 90 dnech. Tato výjimka je spjata se službou informování o platebním účtu, kdy uživatel autorizuje přístup aplikace třetí strany ke svému platebnímu účtu. Každých 90 dní musí uživatel potvrdit, že trvá jeho vůle o souhlasu se získáváním těchto výše uvedených údajů.[231]

Dle mého názoru se mi tato lhůta na potvrzování zdá velmi nekomfortní pro uživatele užívající aplikace třetích stran. Tyto aplikace mají usnadňovat každodenní fungování uživatelů. Každé oznámení či potvrzení pouze zdržuje, z mé vlastní zkušenosti. Nechal bych rozhodnutí na každém uživateli, zda chce dále sdílet tato data s poskytovateli služby informování o platebním účtu a spoléhal se na rozumné uvažování těchto uživatelů. Někteří ze širší odborné veřejnosti[232] se obávali toho, zda tento model nebude podporovat BFU (běžného Frantu uživatele) k tomu, aby takový uživatel povolil bezhlavě každé aplikaci přístup k svým datům. Myslím si, že rozumně uvažující člověk bude uvažovat nad tím, komu povolí přístup, a navíc ochrana osobních dat v Evropské unii je již na tak vysoké úrovni, že i kdyby se stalo něco podobného, jak výše prorokovali, tak to nebude mít velké následky.

3.2.2. Bezkontaktní platby v místě prodeje

Výjimka ze silného ověření uživatele v případě bezkontaktní platby v místě prodeje se uplatní, pokud se splní následující podmínky:

„a) jednotlivá částka bezkontaktní elektronické platební transakce nepřesáhne 50 EUR a

b) kumulativní částka předchozích bezkontaktních elektronických platebních transakcí iniciovaných prostřednictvím platebního prostředku s bezkontaktní funkcí ode dne posledního uplatnění silného ověření klienta nepřesáhne 150 EUR, nebo

---

[231] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[232] BREJČÁK, Peter. Startupy zbrzdí regulace a další vzniknou jen pro efekt: 6 rizik, které do bankovnictví přináší PSD2. *Tyinternety* [online]. 2018 [cit. 2021-02-22]. Dostupné z: https://tyinternety.cz/fastnews/6-rizik-ktere-do-bankovnictvi-prinasi-psd2/

c) počet po sobě následujících bezkontaktních elektronických platebních transakcí iniciovaných prostřednictvím platebního prostředku nabízejícího bezkontaktní funkci ode dne posledního uplatnění silného ověření klienta nepřesáhne pět.“[233]

Z těchto podmínek můžeme vyčíst, že silné ověření uživatele není potřeba v případě jednotlivé transakce, která nepřesáhne 50 EUR nebo pokud kumulativní částka všech transakcí od posledního silného ověření uživatele nepřesáhne 150 EUR. Můžeme tomu porozumět tak, že při platbě kartou, kdy se zadává PIN kód, který je zároveň prvkem znalosti a platební karta představuje prvek držení (viz v kapitole 3.1.2.) splní požadavky silného ověření uživatele, pokud přesáhne buď jednotlivá transakce hodnoty 50 EUR nebo 150 EUR při více transakcích.

Vydavatelské banky však vyžadují PIN kód při bezkontaktních platbách nad 500 Kč, dále po určitém počtu transakcí bez použití PIN kódu a někdy jej vyžaduje zcela náhodně. Hranice 500 Kč je nastavená skrze konsensus vydavatelských bank v České republice[234] [235]. Ohledně tohoto limitu se vedly diskuse na začátku pandemie koronaviru COVID-19, ale limity se nezvýšily, navzdory ostatních členských zemí, které tyto limity zvýšily až do výše 50 EUR, které směrnice PSD2 povoluje.[236]

S příchodem Apple Pay na český trh[237] a dalších ekvivalentů v podobě například Garmin Pay či Google Pay, nabývám pocitu, že používání klasických platebních karet už není na pořadu dne a brzo tato výjimka už nebude ani potřeba.

3.2.3. Terminály bez obsluhy pro jízdné a poplatky za parkování

Silné ověření uživatele se nepoužije v případě samoobslužných terminálů na placení jízdného nebo parkovného bez limitu částky či počtu transakcí, jako

---

[233] Článek 11 nařízení Komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace

[234] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[235] SVOBODA, Jakub. PIN při platbě kartou nad 500 korun zůstává, banky zvýšení limitu odmítly. *Novinky.cz* [online]. 2020 [cit. 2021-02-22]. Dostupné z: https://www.novinky.cz/finance/clanek/pin-pri-platbe-kartou-nad-500-korun-zustava-banky-zvyseni-limitu-odmitly-40320375

[236] HOVORKOVÁ, Kateřina. Virus donutil řadu zemí zvýšit limity pro neověřené platby. Česko se však změně brání. *Aktuálně.cz* [online]. 2020 [cit. 2021-02-22]. Dostupné z: https://zpravy.aktualne.cz/finance/rada-zemi-zvysila-limity-pro-platby-kartou-bez-overeni-ceske/r~f9bafb7aac9611ea8b230cc47ab5f122/

[237] MATURA, Jan. PŘEHLEDNĚ: Jak aktivovat Apple Pay a jak jsou platby zabezpečené. *IDNES.cz* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://www.idnes.cz/mobil/tech-trendy/apple-pay-v-cesku-videonavod.A190219_085956_mob_tech_jm

například v kapitole 3.2.2.[238] Se samoobslužnými terminály se dá setkat například v plzeňské MHD (která byla mezi prvními v České republice), kde je možnost zaplatit bezkontaktně jízdenku, dále pak v obchodních domech, kde zákazník zaplatí na výjezdu z parkoviště nebo v parkovacím domě Rychtářka v Plzni.

3.2.4. Důvěryhodní příjemci

Uživatel dle nařízení RTS zde má možnost zařadit u poskytovatele platebních služeb příjemce na seznam důvěryhodných příjemců, u kterých nebude potřeba uplatnění silného ověření klienta při iniciování platební transakce. Při tvorbě tohoto seznamu je ale silné ověření uživatele zapotřebí.[239]

3.2.5. Opakující se transakce

Silné ověření klienta se vždy v těchto případech použije poprvé, kdy uživatel vytváří, změní nebo poprvé iniciuje transakci. Transakce musí mít stejného příjemce a vždy stejnou částku.[240]

Typicky opakující se transakce jsou trvalé příkazy nebo platba za předplatné některých služeb.

3.2.6. Úhrady mezi účty téže fyzické nebo právnické osoby

V případě, že uživatel má u stejného poskytovatele platebních služeb více účtů, například u stejné banky, silné ověření uživatele se neprovede v případě iniciace úhradu z jednoho účtu na druhý. Tato výjimka platí jak pro fyzické, tak i právnické osoby.

3.2.7. Transakce týkající se malých částech

V případě, že uživatel iniciuje elektronickou platební transakci na dálku a splní následující podmínky:

„a) částka elektronické platební transakce na dálku nepřesáhne 30 EUR a

b) kumulativní částka předchozích elektronických platebních transakcí na dálku iniciovaných plátcem ode dne posledního uplatnění silného ověření klienta nepřesáhne 100 EUR, nebo

---

[238] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[239] Ibid.

[240] Článek 14 nařízení Komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace

c) počet předchozích elektronických platebních transakcí na dálku iniciovaných plátcem od posledního uplatnění silného ověření klienta nepřesáhne pět po sobě následujících jednotlivých elektronických platebních transakcí na dálku.“[241]

Při elektronické platební transakci na dálku, která je do částky 30 EUR, a tedy je bez silného ověření klienta, poskytovatel platebních služeb si vybere jednu z dvou možností, které mu nařízení RTS dává.

3.2.8. Zabezpečené platební procesy a protokoly společností

Tato výjimka platí pro uživatele, kteří jsou právnickými osobami a nejsou spotřebiteli. Tyto právnické osoby „iniciují elektronické platební transakce použitím zvláštních platebních procesů nebo protokolů, které jsou zpřístupněny pouze plátcům, kteří nejsou spotřebiteli“[242] což můžeme chápat, jako „korporátní společnosti (nikoliv spotřebitelé) a kde je zabezpečení dosaženo jinými prostředky než autentizací jednotlivé osoby“[243].

3.2.9. Analýza transakčních rizik

Předposlední výjimka, při které poskytovatel platebních služeb nemusí použít silné ověření klienta, nastane v případě, kdy identifikuje transakci s nízkou mírou rizika na základě toho, když berou v potaz rizikové faktory, jako jsou seznamy odcizených či vyzrazených ověřovacích prvků, částky platebních transakcí, scénáře podvodů při poskytování platebních služeb, napadení malwarem při spojení během ověření nebo třeba neobvyklé použití zařízení nebo softwaru pro přístup.[244]

S výše uvedenými případy musí poskytovatel platebních služeb kombinovat také referenční hodnoty pro „elektronické karetní platby na dálku“, resp. „elektronické úhrady na dálku“[245] v příloze nařízení RTS o míře podvodů, částky transakce, které nepřesahují stanovenou hodnotu pro výjimku v těchto tabulkách a zda v reálném čase nezjistil během analýzy rizik neobvyklé chování plátce či

---

[241] Článek 16 Nařízení Komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace

[242] Článek 17 Ibid.

[243] HUML, Tomáš. PSD2: Finální verze RTS k SCA – shrnutí zásadních změn. In: *Deloitte Česká republika* [online]. 2017 [cit. 2021-02-22]. Dostupné z: https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/Deloitte_PSD2_Final_RTS_k_SCA_Souhrn_zasadnich_zmen_Technolog_Security.pdf

[244] Článek 2, odst. 2 Nařízení Komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace

[245] Článek 18, odst. 2 Ibid.

výdaje, neobvyklé informace o zařízení nebo softwaru plátce, napadení malwarem při spojení během ověření, neobvyklé místo plátce, známé scénáře podvodů při poskytování platebních služeb a vysoce rizikové místo příjemce.[246]

3.2.10. Výpočet míry podvodů

Součástí nařízení RTS je pro každý druh transakce v příloze celková míra podvodů, která se vztahuje na platební transakce ověřené silným ověřením uživatele.[247] V případě, že míra podvodů přesáhne referenční hodnoty v příloze, poskytovatel platební služby musí vyrozumět ČNB a pokud překročí ve dvou po sobě jdoucí čtvrtletí, nelze výjimky ze silného ověření uživatele nadále využít.[248]

3.3. Porušení povinnosti

Pokud poskytovatel platebních služeb neprovede silné ověření uživatele, ve výše již zmíněných případech, kdy je zapotřebí jej provést, při vzniku škody za neautorizovanou platební transakci, pak nese ztrátu poskytovatel platebních služeb v plné výši.[249]

Při porušení povinnosti ze strany uživatele, například vyzrazení prvků a faktorů silného ověření uživatele, nese uživatel ztrátu z neautorizované platební transakce.[250] Více o porušení povinnosti ze strany uživatele v kapitole 4.

---

[246] Článek 18, odst. 2 Nařízení Komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace

[247] Článek 19, odst. 1 Ibid.

[248] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[249] § 182, odst. 3, písm. c) zákona č. 370/2017 Sb., o platebním styku

[250] NÝDRLE, Tomáš. § 223 [*Vymezení a použití silného ověření uživatele*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

4. Snížení limitu odpovědnosti plátce při neautorizované platební transakci

V návaznosti na ustanovení článku 74 směrnice PSD2, snížil český zákonodárce spoluúčast plátce na částku 50 EUR[251] oproti původní částce 150 EUR ZoPS z roku 2009[252], kterou musí nést plátce z neautorizované platební transakce v některých případech, které níže uvedu. zajímavostí je, že tato novinka byla často uváděna mezi hlavními přínosy směrnice PSD2.[253]

Neautorizovaná platební transakce není přímo definovaná v ZoPS, avšak logickým výkladem argumentum a contrario ustanovení § 156 ZoPS můžeme vyvozovat, že neautorizovaná platební transakce je platební transakce, ke které plátce nedal souhlas. Mezi neautorizovanou platební transakcí můžeme řadit platební transakce provedená jinou osobou, která použila či zneužila ztracený nebo odcizený platební prostředek.[254] Dále „platební transakce, k níž plátce udělil souhlas neplatně (např. pro nedostatek svobody vůle, srozumitelnosti nebo určitosti jejího projevu, případně pro nezpůsobilost plátce souhlas s platební transakcí udělit nebo pro nedodržení dohodnuté formy), platební transakce, k níž plátce udělil souhlas, ale následně jej platně odvolal (srov. § 157), platební transakce opakovaná, ačkoli plátce udělil souhlas pouze k jedné platební transakci.“[255]

Pokud proběhne neautorizovaná platební transakce, poskytovatel buď oznámí plátci nebo plátce oznámí poskytovateli o takové skutečnosti. Poskytovatel má následně dva scénáře, jak se zachovat. Ustanovení § 182, odst. 1, písm. a) ZoPS hovoří o „uvede platební účet, z něhož byla částka platební transakce odepsána, do stavu, v němž by byl, kdyby k tomuto odepsání nedošlo“, čemuž rozumím jako vrácení částky, která byla předmětem neautorizované platebním transakce zpět na platební účet s čím se ztotožňují i autoři komentáře k ZoPS[256]. V případě, že není možná tímto způsobem, například tím, že neměl založený platební účet nebo mu

[251] § 182, odst. 1, písm. a) zákona č. 370/2017 Sb., o platebním styku

[252] § 116, odst. 1, písm. a) Ibid.

[253] Platby po internetu mají být bezpečnější, nová pravidla schválila vláda. *Aktuálně.cz* [online]. 2017 [cit. 2021-03-15]. Dostupné z: https://zpravy.aktualne.cz/finance/platby-po-internetu-maji-byt-bezpecnejsi-nova-pravidla-schva/r~df8c3efe07d911e78af8002590604f2e/

[254] § 182, odst. 1, písm. a) Ibid.

[255] BERAN, Jiří. § 182 [*Výjimky z povinnosti napravit neautorizovanou platební transakci*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[256] Ibid.

byl zrušen.[257] Poskytovatel musí vrátit „částku platební transakce, zaplacenou úplatu a ušlé úroky plátci“[258].

V některých případech neautorizované platební transakce nese plátce určitou část ze ztráty, která mu vznikne. Výše uvedená proklamace snížení spoluúčasti za ztrátu z 150 EUR na 50 EUR platí v případě, že plátce ztratí nebo, mu byl odcizen nebo zneužit jeho platební prostředek. Platebním prostředkem může být například platební karta.[259]

Ústavní soud v judikátu I. ÚS 1833/18, vyložil pojem ztráta následovně: „Slovo ztratit znamená skutečně pozbytí možnosti s věcí nakládat, nicméně bez zjevného úmyslu vlastníka či držitele, což uvedl i Nejvyšší a městský soud. Od toho je však třeba odlišit situace, kdy vlastník nebo držitel ztrácejí momentální dispozici, kdy věc je předmětem právního poměru. V těchto situacích je vlastníku či držiteli známo, kde se věc nachází, a předpokládá její navrácení či jiný, zpravidla sjednaný, smluvní osud“[260].[261]

Pojem odcizení můžeme v tomto případě chápat jako „odnětí platebního prostředku“[262]. Pojem zneužití je podle komentáře k ZoPS širším pojmem než ztráta a odcizení, jelikož zneužití může nastat i v případě, že je platební prostředek stále v dispoziční sféře plátce. Perfektním příkladem zneužití se zdá být zkopírování údajů z platební karty.[263]

V případě, že plátce nejedná podvodně, což znamená „úmyslné uvedení poskytovatele v omyl, využití jeho omylu nebo zamlčení podstatných skutečností“[264], můžou nastat výjimky, kdy nemusí nést spoluúčast na ztrátě. Výjimka nastává v případě, že nezjistil „ztrátu, odcizení nebo zneužití platebního

[257] BERAN, Jiří. § 181 [*Povinnost napravit neautorizovanou platební transakci*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[258] § 181, odst. 1, písm. b) zákona č. 370/2017 Sb., o platebním styku.

[259] BERAN, Jiří. § 182 [*Výjimky z povinnosti napravit neautorizovanou platební transakci*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[260] Nález Ústavního soudu ze dne ze dne 06.02.2020, sp. zn. I. ÚS 1833/18.

[261] BERAN, Jiří. § 182 [*Výjimky z povinnosti napravit neautorizovanou platební transakci*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[262] Ibid.

[263] Ibid.

[264] Ibid.

prostředku“[265], na danou výjimku jsou různé názory. Například autoři komentáře k ZoPS tvrdí, že může nastat v případě, že zloděj cestujícímu v tramvaji ukradne peněženku s platební kartou a použije jej.[266] Cestující to zjistí až později a nahlásí ztrátu. K této variantě se přikláním i já. V případě, že nastane „ztráta, odcizení nebo zneužití platebního prostředku byla způsobena jednáním poskytovatele“[267], plátce nemusí nést spoluúčast na ztrátě.

Pokud plátce způsobí ztrátu z neautorizované platební transakce svým podvodným jednáním, úmyslně či hrubou nedbalostí tak, že poruší povinnosti ochrany jeho osobních bezpečnostních prvků, které vyplývají z rámcové smlouvy s poskytovatelem[268] nebo následného oznámení pro „ztrátu, odcizení, zneužití nebo neoprávněné použití platebního prostředku“[269].

Ustanovení § 182 ZoPS o uplatnění ztráty z neautorizovaných platebních transakcí se zcela nepoužije v případě, že plátce nejednal podvodně, splnil informační povinnost ohledně oznámení ztráty, odcizení nebo zneužití [270], poskytovatel nepožadoval silné ověření uživatele, když byl povinen [271] a v neposlední řadě, když poskytovatel nezajistí vhodné prostředky k oznámení ztráty, odcizení nebo zneužití platebního prostředku.[272]

Jestliže neautorizovaná platební transakce proběhla s elektronickými penězi, „jejichž povaha poskytovateli neumožňuje zabránit jejich jakémukoli užití“[273], nese ztrátu plátce. Mezi známé elektronické peníze patří „např. Ecash, Cybercash, Milcent a Mondex“[274].

Elektronické peníze jsou definovány v ustanovení § 4 ZoPS jako „peněžní hodnota, která

---

[265] § 182, odst. 2, písm. a) zákona č. 370/2017 Sb., o platebním styku.

[266] BERAN, Jiří. § 182 [*Výjimky z povinnosti napravit neautorizovanou platební transakci*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[267] § 182, odst. 2, písm. b) zákona č. 370/2017 Sb., o platebním styku

[268] BERAN, Jiří. § 182 [*Výjimky z povinnosti napravit neautorizovanou platební transakci*]. In: BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

[269] § 165, písm. b) zákona č. 370/2017 Sb., o platebním styku

[270] § 182, odst. 3, písm. a) Ibid.

[271] § 182, odst. 3, písm. c) Ibid.

[272] § 182, odst. 3, písm. b) Ibid.

[273] § 182, odst. 4 zákona Ibid.

[274] POSPÍŠIL, Lukáš. Elektronické peníze versus Kryptoměna. *Epravo.cz* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://www.epravo.cz/top/clanky/elektronicke-penize-versus-kryptomena-107930.html

a) představuje pohledávku vůči tomu, kdo ji vydal,

b) je uchovávána elektronicky,

c) je vydávána proti přijetí peněžních prostředků za účelem provádění platebních transakcí a

d) je přijímána jinou osobou než tím, kdo ji vydal.“[275]

[275] § 4, odst. 1 zákona č. 370/2017 Sb., o platebním styku

Závěr

Cílem mé diplomové práce bylo představit vybrané novinky a nové služby, které přišly s platností nového zákona o platebním styku, jak jsou tyto novinky a služby implementovány do našeho právní řádu ze směrnice PSD2 a následně jak jsou v praxi používány.

Českou republiku jsem vždy vnímal za průkopníka v IT oblasti, zejména v bankovnictví a zavádění novinek v oblasti FinTech, ale reálný pohled na právní řád a vnímání hráčů na trhu mě trochu vyvedl z tohoto obrazu, který jsem měl v sobě zastával. Překvapila mě délka řízení povolení k činnosti u správců informací o platebním účtu, o platebních institucí nevyjímaje.

Od Open banking jsem si sliboval mnohé, zejména to, že přinese nové služby na náš trh, ale z poznatků, které jsem nabyl, mám pocit, že třetí strany nejsou spokojené s dosavadním fungováním a nefunguje v praxi tak, jak by měl a má daleko k tomu, jak si to usmyslel evropský zákonodárce. Myslím si, že směrnice PSD3 v tomto směru bude chtít harmonizovat open banking standardy a odstraní tak jednu z překážek pro nové FinTech společnosti/start-upy, které nemusí mít dostatek finančních prostředků k přístupu na další trhy v členských státech s odlišným pojením open banking standardu a odstraní tím zmatky v API.

Potvrdil jsem si výzkumy, že multibanking aplikace jsou pro velmi úzkou část uživatelů a nejsem to pouze já, který je skeptický z hlediska bezpečnosti a užitečnosti této funkce. Překvapila mě však ta skutečnost, že čeští uživatelé jsou velmi konzervativními v porovnání s východní Evropou. S počtem bezkontaktních platebních terminálů a vydaných bezkontaktních karet (po uvedení na trh) v České republice jsem nabyl pocitu, že čeští uživatelé mají rádi nové technologické novinky a nezdráhají se jich zkoušet, byť riziko neautorizované platební transakce tu bylo vždy.

Silnému ověření uživatele jsem věnoval kvantum času, jelikož mě prvky ověření fascinovaly už předtím, než jsem vůbec uvažoval nad tím, že budu psát svou diplomovou práci o tématu spojeném se směrnicí PSD2. Vždy mě zajímal prvek inherence, a to jak z technického, tak i právního hlediska. Využití hlasu člověka k jeho rozpoznání jsem často považoval za nereálné, ovšem až do března tohoto roku, kdy jsem měl šanci jej konečně využít, především díky rešerši na dané

téma. Netušil jsem však, že existuje tolik výjimek ze silného ověření uživatele, avšak mě nemile překvapila lhůta u výjimky informování o platebním účtu.

Na závěr jsem se zabýval snížením limitu odpovědnosti plátce, což bylo hojně diskutovaným tématem při zavedení zákona o platebním styku v roce 2018. Velmi mě překvapilo, kolik výjimek v odpovědnosti plátce lze v zákoně o platebním styku najít.

Během rešerše a psaní této diplomové práce jsem nabyl pocitu, že směrnice PSD2 byl průkopníkem v době schválení, ale s postupem času zestárla a je potřeba přijít s novým směrem vývoje platebního styku napříč Evropou a podchytit začátky zajímavých služeb, které můžou být v budoucnu nedílnou součástí našich životů. Ostatně openFinance Framework z dílny Berlin Group chce zavést nové služby nad rámec PSD2 a jsem zvědav, zda ve směrnici PSD3 převezme zákonodárce právě Open banking standard od Berlin Group, která je nejvíce rozšířená v celé Evropě.

Velice se těším na budoucnost bankovnictví, kterou nám přinese Evropská unie s další směrnicí PSD3 či jinými regulacemi napříč členskými státy a zejména na FinTech společnosti, s jakými službami přijdou v následujících letech v post-covidovém období.

Resumé

The subject of this diploma thesis is "Selected issues of the Act on Payments in relation with PSD2". The primary goal of this thesis is to introduce selected new regulations from the Act on Payments in relation with the Payment Services Directive 2 (PSD2) and primary focused on the innovations, which can be helpful for FinTech sector. The secondary goal of this thesis is to provide preview, how these innovations are used among users and FinTech companies or another entity (banks, etc.). The diploma thesis is divided to four chapters.

The first chapter is about PSD2 and its new regulations. It also describes how they were implemented into the Act on Payments and points out changes compared to the PSD from 2007.

The second chapter focus on FinTech and its use of new regulations in connection with PSD2. In this chapter the new services are described such as Account Information Service (AIS) or Payment Initiation Service (PIS). It also provides introduction into Open Banking platform and description of two association, which are important for FinTech scene in the Czech Republic. The end of chapter is focus to the application, which use new services as AIS and PIS.

The third chapter is about Strong Customer Authentication, which is one of the regulatory frameworks, which set the new level of security for payment on the Internet.

The last chapter is dedicated to the reduction of the payer's liability for unauthorized payment transactions, regarding to the conditions which the payer will not bear any financial losses and those case where the payer will bear all financial losses.

Seznam použité literatury

Odborné publikace

BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. Zákon o platebním styku: Komentář [Systém ASPI]. *Wolters Kluwer* [cit. 2021-3-11]. ASPI_ID KO370_2017CZ. Dostupné v Systému ASPI. ISSN: 2336-517X.

PETROV, Jan, Michal VÝTISK a Vladimír BERAN. Občanský zákoník: komentář. 2. vydání. V Praze: *C.H. Beck*, 2019. Beckova edice komentované zákony. ISBN 978-80-7400-747-7.

Právní předpisy a podzákonné předpisy

Zákon č. 370/2017 Sb., o platebním styku (Zákon o platebním styku)

Zákon č. 500/2004 Sb., o správním řádu (Správní řád)

Zákon č. 89/2012 Sb., občanský zákoník

Zákon č. 634/2004 Sb., o správních poplatcích

Vyhláška č. 1/2018 Sb., o žádostech a oznámeních k výkonu činnosti podle zákona o platebním styku

Vyhláška č. 7/2018 Sb., o některých podmínkách výkonu činnosti platební instituce, správce informací o platebním účtu, poskytovatele platebních služeb malého rozsahu, instituce elektronických peněz a vydavatele elektronických peněz malého rozsahu

Úřední sdělení České národní banky č. 18/2020 Věst. ČNB ze dne 5. srpna 2020 k výkladu pojmů důvěryhodnost a odborná způsobilost

Důvodová zpráva k zákonu č. 370/2017 Sb. o platebním styku, č. 370/2017 Dz

European Banking Authority. EBA-Op-2018-04: Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC ze dne 13. června 2018.

European Banking Authority. EBA-Op-2019-06: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 ze dne 21. června 2019.

Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES,

2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES

Směrnice Evropského parlamentu a Rady 2007/64/ES ze dne 13. listopadu 2007 o platebních službách na vnitřním trhu

Nařízení Komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace

Nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro bankovnictví), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/78/ES

Elektronické prameny

1. PF Finance, s.r.o. [online]. [cit. 2021-03-16]. Dostupné z: https://www.1pffin.cz/

AIS and PIS – A status update on open banking licenses issued in the UK. *Penser* [online]. 05.2019n. l. [cit. 2021-03-07]. Dostupné z: https://www.penser.co.uk/business/ais-and-pis-a-status-update-on-the-licenses-issued-in-the-uk/

BACHURA, Jan. S aplikací George klíč lze nově potvrzovat i platby na internetu. Jak budou moct klienti v roce 2021 potvrzovat platby kartou v eshopech? *Finparáda* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://www.finparada.cz/6688-S-aplikaci-George-klic-lze-nove-potvrzovat-i-platby-na-internetu.aspx

BARANOVÁ, Iva a Linda KOLAŘÍKOVÁ. PSD2: novelizace platebních služeb. *KPMG Česká republika* [online]. 2017 [cit. 2021-03-01]. Dostupné z: https://danovky.cz/cs/psd2-novelizace-platebnich-sluzeb

BARTÁČEK, Václav. Představení PSD2 nejen pro vývojáře. Blíží se otevřené bankovnictví? Udělejte si v tom jasno. *Zdroják.cz* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://zdrojak.cz/clanky/psd2-nejen-pro-vyvojare/

BEDRICH, Vaclav. Český fintech Spendee získal od ČNB jako první licenci k přímému propojení s bankami. *CzechCrunch* [online]. 2018 [cit. 2021-02-22].

Dostupné z: https://www.czechcrunch.cz/2018/12/cesky-fintech-spendee-ziskal-od-cnb-jako-prvni-licenci-k-primemu-propojeni-s-bankami/

BREJČÁK, Peter. Přichází revoluční PSD2: Jak se změní svět fintech startupů? *Tyinternety* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://tyinternety.cz/startupy-a-byznysy/prichazi-revolucni-psd2-se-zmeni-svet-fintech-startupu/

BREJČÁK, Peter. Startupy zbrzdí regulace a další vzniknou jen pro efekt: 6 rizik, které do bankovnictví přináší PSD2. *Tyinternety* [online]. 2018 [cit. 2021-02-22]. Dostupné z: https://tyinternety.cz/fastnews/6-rizik-ktere-do-bankovnictvi-prinasi-psd2/

BUBÁK, Zdeněk. Český standard pro Open Banking je na světě. *Finparáda* [online]. 2017 [cit. 2021-03-15]. Dostupné z: https://www.finparada.cz/mobile/4722-Cesky-standard-pro-Open-Banking-je-na-svete.aspx

BUCHBAUER, Petr. Dveře pro nové finanční služby se otevírají aneb průvodce tajemnou PSD2. *Peak.cz* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://www.peak.cz/dvere-nove-financni-sluzby-se-otviraji-aneb-pruvodce-tajemnym-psd2/8841/

BUŘÍNSKÁ, Barbora. Klienti se přesouvají do onlinu, velké banky zavírají pobočky. *Novinky.cz* [online]. 2020 [cit. 2021-02-22]. Dostupné z: https://www.novinky.cz/finance/clanek/klienti-se-presouvaji-do-onlinu-velke-banky-zaviraji-pobocky-40340316

Co je to API (application programming interface)? *Topranker.cz* [online]. [cit. 2021-03-15]. Dostupné z: https://topranker.cz/slovnik/co-je-to-api-application-programming-interface/

Co PSD1 a PSD2 znamenají a proč jsou důležité? *IBanFirst Blog* [online]. 2018 [cit. 2021-03-16]. Dostupné z: https://blog.ibanfirst.com/cz/co-psd1-a-psd2-znamenaj%C3%AD-a-pro%C4%8D-jsou-d%C5%AFle%C5%BEit%C3%A9

ČERMÁK, Jan. Novinky v oblasti silného ověření uživatele. *Právní prostor* [online]. 2021 [cit. 2021-03-15]. Dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/novinky-v-oblasti-silneho-overeni-uzivatele

Česká spořitelna spouští aplikaci George klíč pro všechny klienty. *Česká spořitelna* [online]. 2019 [cit. 2021-02-23]. Dostupné z: https://www.csas.cz/cs/o-nas/pro-media/tiskove-zpravy/2019/09/11/ceska-sporitelna-spousti-aplikaci-george-klic-pro-vsechny-klienty

Český standard pro Open banking. *Česká bankovní asociace* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/cesky-standard-pro-open-banking

Češi a digitalizace 2019. *Česká bankovní asociace* [online]. 2019 [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/cesi-a-digitalizace-2019

Češi a digitalizace 2020. *Česká bankovní asociace* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/cesi-a-digitalizace-2020

Členové asociace. *Česká bankovní asociace* [online]. [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/clenove

DONÁT, Josef. Směrnice PSD2 a revoluce v platebních službách. *Epravo.cz* [online]. 2016 [cit. 2021-02-22]. Dostupné z: https://www.epravo.cz/top/aktualne/smernice-psd2-a-revoluce-v-platebnich-sluzbach-102716.html

DOSKOČILOVÁ, Veronika. PSD2 rok poté: multibanking umí 5 bank, API nezpřístupnila polovina. *Měšec.cz* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://www.mesec.cz/clanky/psd2-rok-pote-multibanking-umi-5-bank-api-nezpristupnila-polovina/

EISELT, Zbyněk. Co znamená silné ověření klienta (SCA) a proč se o něm všude mluví? *GoPay blog* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://www.gopay.com/blog/co-znamena-silne-overeni-klienta-sca-a-proc-se-o-nem-vsude-mluvi/

Evropský průzkum Deloitte ke směrnici PSD2. *Deloitte Česká republika* [online]. [cit. 2021-03-15]. Dostupné z: https://www2.deloitte.com/cz/cs/pages/financial-services/articles/deloitte-european-psd2-surveys.html

Facebook přiznal obří únik dat. Útočníci se dostali k 50 milionům uživatelských účtů. *INFO.CZ* [online]. 2018 [cit. 2021-02-22]. Dostupné z: https://www.info.cz/zpravodajstvi/svet/facebook-priznal-obri-unik-dat-utocnici-se-dostali-k-50-milionum-uzivatelskych-uctu

FALTOVÁ, Nikola. Nový zákon o platebním styku a největší změny, které přináší. *Epravo.cz* [online]. 2017 [cit. 2021-03-01]. Dostupné z: https://www.epravo.cz/top/clanky/novy-zakon-o-platebnim-styku-a-nejvetsi-zmeny-ktere-prinasi-106626.html

FAQs. *Open Banking* [online]. [cit. 2021-03-15]. Dostupné z: https://www.openbanking.org.uk/customers/faqs/

FinTech v ČR i ve světě. In: *Deloitte Česká republika* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/FinTech_v_CR_i_ve_svete_v2.pdf

FRYDLEWICZ, Jiří. Otevřené bankovnictví se blíží, klienti si ale na nové funkce počkají. *E15.cz* [online]. 2017 [cit. 2021-02-22]. Dostupné z: https://www.e15.cz/finexpert/investujeme/otevrene-bankovnictvi-se-blizi-klienti-si-ale-na-nove-funkce-pockaji-1341003

HINGAR, Petr. Otevřené bankovnictví, PSD2, open API a BankID aneb Změna paradigmatu ve finančním sektoru. *SystemOnline.cz* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://www.systemonline.cz/it-pro-banky-a-financni-organizace/otevrene-bankovnictvi-psd2-open-api-a-bankid.htm

HORÁČEK, Jakub. Speciální hesla či biometrické údaje. Začínají platit přísnější pravidla pro platby po internetu. *IROZHLAS* [online]. 2019 [cit. 2021-03-15]. Dostupné z: https://www.irozhlas.cz/ekonomika/platby-pres-internet-nakupovani-online-zmena-pravidel_1909140630_kro

HOVORKOVÁ, Kateřina. Virus donutil řadu zemí zvýšit limity pro neověřené platby. Česko se však změně brání. *Aktuálně.cz* [online]. 2020 [cit. 2021-02-22]. Dostupné z: https://zpravy.aktualne.cz/finance/rada-zemi-zvysila-limity-pro-platby-kartou-bez-overeni-ceske/r~f9bafb7aac9611ea8b230cc47ab5f122/

How to import data? *Spendee Help Center* [online]. [cit. 2021-02-22]. Dostupné z: https://help.spendee.com/article/121-import-transactions

HUML, Tomáš. PSD2: Finální verze RTS k SCA – shrnutí zásadních změn. In: *Deloitte Česká republika* [online]. 2017 [cit. 2021-02-22]. Dostupné z: https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-

services/Deloitte_PSD2_Final_RTS_k_SCA_Souhrn_zasadnich_zmen_Technolog_Security.pdf

Jak se staví evropské finanční právo k FinTech firmám? *Konečná & Zacha: Advokátní kancelář* [online]. [cit. 2021-02-22]. Dostupné z: https://www.konecna-zacha.com/jak-se-stavi-evropske-financni-pravo-k-fintech-firmam-/

Jak prosperovat v nejisté době. In: *Deloitte Česká republika* [online]. 2017 [cit. 2021-03-15]. Dostupné z: https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-otevrene-bankovnictvi-a-psd2.pdf

Jsou otevřená data příležitostí pro banky? Největší festival nad otevřenými daty v ČR. *Česká spořitelna* [online]. 2017 [cit. 2021-03-15]. Dostupné z: https://www.csas.cz/cs/o-nas/pro-media/tiskove-zpravy/2017/11/23-1/nejvetsi-festival-nad-otevrenymi-daty-v-cr

Kdo jsme a co děláme. *Česká bankovní asociace* [online]. [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/co-delame

Komerční banka spolupracuje s BudgetBakers. In: *Komerční banka* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://www.kb.cz/cs/o-bance/pro-media/tiskove-zpravy-2019/komercni-banka-spolupracuje-s-budgetbakers

KŘÍŽ, Lukáš a David ZAJÍC. PSD2: malá revoluce v platebních službách. *Hospodářské noviny* [online]. [cit. 2021-03-16]. Dostupné z: https://ictrevue.ihned.cz/c3-65786220-0ICT00_d-65786220-psd2-mala-revoluce-v-platebnich-sluzbach

LANGEROVÁ, Jana. Co přinese novela o platebním styku? Žádné revoluční změny. *Podnikatel.cz* [online]. 2020 [cit. 2021-03-16]. Dostupné z: https://www.podnikatel.cz/clanky/co-prinese-novela-o-platebnim-styku-zadne-revolucni-zmeny/#h20

LANGEROVÁ, Jana. Je multibanking výhodou, nebo jen trendem? Zjistěte, kdo ho klientům nabízí. *Podnikatel.cz* [online]. 2019 [cit. 2021-03-15]. Dostupné z: https://www.podnikatel.cz/clanky/je-multibanking-vyhodou-nebo-jen-trendem-zjistete-kdo-jej-klientum-nabizi/

LEIXNEROVÁ, Lucie. PSD2: z jediné aplikace do všech bank bez rizika. *Světchytře.cz* [online]. 2018 [cit. 2021-03-14]. Dostupné z:

https://www.svetchytre.cz/a/iji3L/psd2-z-jedine-aplikace-do-vsech-bank-bez-rizika

MATURA, Jan. PŘEHLEDNĚ: Jak aktivovat Apple Pay a jak jsou platby zabezpečené. *IDNES.cz* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://www.idnes.cz/mobil/tech-trendy/apple-pay-v-cesku-videonavod.A190219_085956_mob_tech_jm

MLADĚNKA, Václav. PSD2 a (r)evoluce bankovnictví. *CFOworld.cz* [online]. 2020 [cit. 2021-03-16]. Dostupné z: https://www.cfoworld.cz/clanky/psd2-a-r-evoluce-bankovnictvi/

MOSNÁKOVÁ, Michaela. PSD2 a nová platební služba: Nepřímé udělení platebního příkazu. *Epravo.cz* [online]. 2018 [cit. 2021-03-06]. Dostupné z: https://www.epravo.cz/top/clanky/psd2-a-nova-platebni-sluzba-neprime-udeleni-platebniho-prikazu-107127.html

Multibanking 2021: Jak funguje a které banky ho podporují? *Skrblík.cz* [online]. [cit. 2021-03-15]. Dostupné z: https://www.skrblik.cz/finance/ucty/multibanking/

Naše projekty. *Česká bankovní asociace* [online]. [cit. 2021-03-15]. Dostupné z: https://cbaonline.cz/nase-projekty

NOVÁKOVÁ, Jolana. Otevřené bankovnictví: proč pouštět k penězům na účtu někoho cizího. *IDNES.cz* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://www.idnes.cz/finance/financni-radce/finance-radce-otevrene-bankovnictvi-bezpeci-ochrana.A180215_124706_viteze_kho

Novela poskytování služeb. *Euro.cz* [online]. [cit. 2021-03-16]. Dostupné z: https://www.euro.cz/archiv/novela-poskytovani-sluzeb-823214

NÝDRLE, Tomáš. Co přináší nový zákon o platebním styku? *Právní rádce* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://pravniradce.ihned.cz/c1-66010790-co-prinasi-novy-zakon-o-platebnim-styku

Otisky prstů i osobní údaje. Bezpečnostní firma nechala na internetu 23 gigabytů nechráněných dat. *IROZHLAS* [online]. [cit. 2021-02-22]. Dostupné z: https://www.irozhlas.cz/veda-technologie/hash-otisky-prstu-rozpoznani-obliceje-unik-dat-databaze-guardian-kauza-vedci_1908160800_mpr

PACHOLET, Martin. Stav multibankingu v ČR. *#fintechcowboys.cz* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://fintechcowboys.cz/stav-multibankingu-v-cr/

Platby po internetu mají být bezpečnější, nová pravidla schválila vláda. *Aktuálně.cz* [online]. 2017 [cit. 2021-03-15]. Dostupné z: https://zpravy.aktualne.cz/finance/platby-po-internetu-maji-byt-bezpecnejsi-nova-pravidla-schva/r~df8c3efe07d911e78af8002590604f2e/

POLÁK, Peter. Komentář: PSD2 jako inovace na úkor bezpečnosti? *Tyinternety* [online]. 2018 [cit. 2021-02-22]. Dostupné z: https://tyinternety.cz/technologie/komentar-psd2-jako-inovace-na-ukor-bezpecnosti/

POSPÍŠIL, Lukáš. Elektronické peníze versus Kryptoměna. *Epravo.cz* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://www.epravo.cz/top/clanky/elektronicke-penize-versus-kryptomena-107930.html

PSD2 – Proč Se Divit. *Freefintech.cz* [online]. 2017 [cit. 2021-02-22]. Dostupné z: https://www.freefintech.cz/index.php/2017/12/10/psd2-proc-se-divit/

PRESS RELEASE - Berlin Group starts new openFinance API Framework. *The Berlin Group* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://www.berlin-group.org/single-post/press-release-berlin-group-starts-new-openfinance-api-framework

PROCHÁZKA, Jan. PSD2 a GDPR: Harmonie, či disonance? *Právní rádce* [online]. 2017 [cit. 2021-03-15]. Dostupné z: https://pravniradce.ihned.cz/c1-65909940-psd2-a-gdpr-harmonie-ci-disonance

První česká multibankovní aplikace Richee. Pro CREDITAS ji vytvořila česká IT společnost Cleverlance. *Cleverlance* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://www.cleverlance.de/cz/novinky/Stranky/Richee.aspx

Příležitost s názvem PSD 2. *Deloitte Česká republika* [online]. [cit. 2021-03-15]. Dostupné z: https://www2.deloitte.com/cz/cs/pages/legal/articles/psd2.html

PSD2 Access to Bank Accounts. *The Berlin Group* [online]. [cit. 2021-03-15]. Dostupné z: https://www.berlin-group.org/psd2-access-to-bank-accounts

PSD 2 a nebankovní poskytovatelé po dvou letech – reakce ČNB. *Česká národní banka* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://www.cnb.cz/cs/verejnost/servis-pro-media/autorske-clanky-rozhovory-s-predstaviteli-cnb/PSD-2-a-nebankovni-poskytovatele-po-dvou-letech-reakce-CNB

PSD2: What you need to know about Screen Scraping and API's. *Yapily* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://www.yapily.com/blog/psd2-screenscraping-apis/

ROSE, Kristýna. Banky vs. FinTech a nová evropská regulace: Ďábel se skrývá v detailu. *Roklen24.cz* [online]. 2017 [cit. 2021-02-22]. Dostupné z: https://roklen24.cz/banky-vs-fintech-a-nova-evropska-regulace-dabel-se-skryva-v-detailu/

RTS and ITS. *Deutsche Börse Group* [online]. [cit. 2021-03-15]. Dostupné z: https://www.mds.deutsche-boerse.com/mds-en/RTS-and-ITS-1339928

Scoring u hypotéky. *Banky.cz* [online]. [cit. 2021-03-16]. Dostupné z: https://www.banky.cz/hypotecni-slovnik/scoring-u-hypoteky/

SECHTER, Jakub. Jak jsou české banky s nástupem PSD2 otevřené svým klientům? *Lupa.cz* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://www.lupa.cz/clanky/jak-jsou-ceske-banky-s-nastupem-psd2-otevrene-svym-klientum/

Silné ověření uživatele u plateb kartou na internetu od 1. 1. 2021. *Česká národní banka* [online]. 2020 [cit. 2021-03-15]. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/vykon-dohledu/upozorneni-pro-verejnost/Silne-overeni-uzivatele-u-plateb-kartou-na-internetu-od-1.-1.-2021/

SOUKAL, Marek. Silné ověření klienta při poskytování platebních služeb. *Epravo.cz* [online]. 2019 [cit. 2021-02-23]. Dostupné z: https://www.epravo.cz/top/clanky/silne-overeni-klienta-pri-poskytovani-platebnich-sluzeb-109952.html

Správci informací o platebním účtu a pobočky zahraničních správců informací o platebním účtu (stav ke dni 02.03.2021). *Základní seznamy subjektů (výsledné sestavy)* [online]. [cit. 2021-03-02]. Dostupné z: https://apl.cnb.cz/apljerrsdad/JERRS.WEB15.BASIC_LISTINGS_RESPONSE_3?p_lang=cz&p_DATUM=02.03.2021&p_hie=HI&p_rec_per_page=25&p_ses_idx=355

Stanovy České fintech asociace, z.s., *Česká fintech asociace* [online]. [cit. 2021-03-15]. Dostupné z: http://czechfintech.cz/wp-content/uploads/2018/01/Stanovy_Ceska_fintech_asociace.pdf

Studie Deloitte: České banky i uživatelé jsou na PSD2 v regionu nejlépe připraveni. *Deloitte Česká republika* [online]. [cit. 2021-03-15]. Dostupné z: https://www2.deloitte.com/cz/cs/pages/press/articles/cze-tz-ceske-banky-i-uzivatele-jsou-na-psd2-v-regionu-nejlepe-pripraveni.html

SVOBODA, Jakub. PIN při platbě kartou nad 500 korun zůstává, banky zvýšení limitu odmítly. *Novinky.cz* [online]. 2020 [cit. 2021-02-22]. Dostupné z: https://www.novinky.cz/finance/clanek/pin-pri-platbe-kartou-nad-500-korun-zustava-banky-zvyseni-limitu-odmitly-40320375

ŠOVAR, Jan a Ondřej MIKULA. FinTech v Česku: Legislativní iniciativa míří výlučně z Bruselu. *Právní rádce* [online]. 2017 [cit. 2021-02-22]. Dostupné z: https://pravniradce.ihned.cz/c1-65872700-fintech-v-cesku-legislativni-iniciativa-miri-vylucne-z-bruselu

TÓTHOVÁ, Lucia. Jak těžké je získat PSD2 licenci? *#fintechcowboys.cz* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://fintechcowboys.cz/rozhovor-jak-tezke-je-ziskat-psd2-licenci/

VÁCLAVÍK, Radek. Multibanking: bankovní řešení rok a půl po PSD2. *Trask* [online]. 2019 [cit. 2021-03-15]. Dostupné z: https://www.trask.cz/publikace/multibanking-bankovni-reseni-rok-a-pul-po-psd2

VÁCLAVÍK, Radek. Stav PSD2 v českých bankách. *OpenAPI portál* [online]. 2018 [cit. 2021-03-15]. Dostupné z: https://www.apiportal.cz/novinky/stav-psd2-v-ceskych-bankach/

VEJVODOVÁ, Alžběta. Platební revoluce se nekoná. O licence na nové služby není v Česku zájem. *Právní rádce* [online]. 2018 [cit. 2021-02-22]. Dostupné z: https://pravniradce.ihned.cz/c1-66152590-platebni-revoluce-se-nekona-o-licence-na-nove-sluzby-neni-v-cesku-zajem

VOJTĚCH, Petr. Nový zákon o platebním styku v platnosti. *Epravo.cz* [online]. 2017 [cit. 2021-03-16]. Dostupné z: https://www.epravo.cz/top/clanky/novy-zakon-o-platebnim-styku-v-platnosti-106689.html?mail

Výpis ze spolkového rejstříku - Česká fintech asociace, z.s., L 66392 vedená u Městského soudu v Praze. *Veřejný rejstřík a sbírka listin* [online]. [cit. 2021-03-15]. Dostupné z: https://or.justice.cz/ias/ui/rejstrik-firma.vysledky?subjektId=944463&typ=PLATNY

ZÁMEČNÍKOVÁ, Inka a Konstantin LAVRUSHIN. FinTech část I. – definice a subjekty. *Epravo.cz* [online]. 2017 [cit. 2021-02-22]. Dostupné z: https://www.epravo.cz/top/clanky/fintech-cast-i-definice-a-subjekty-106711.html

ZATLOUKAL, Jiří. Pokračuje propouštění v bankách. Komerčka se zbaví čtvrtiny zaměstnanců. *Seznam Zprávy* [online]. 2021 [cit. 2021-02-22]. Dostupné z: https://www.seznamzpravy.cz/clanek/pokracuje-propousteni-v-bankach-komercka-se-zbavi-ctvrtiny-zamestnancu-142061

Judikatura

Nález Ústavního soudu ze dne ze dne 06.02.2020, sp. zn. I. ÚS 1833/18.

Usnesení Nejvyššího soudu ze dne 24.02.2009, sp. zn. 29 Cdo 4993/2008.

Usnesení Nejvyššího soudu ze dne 26.05.2009, sp. zn. 29 Cdo 1680/2009.

Usnesení Nejvyššího soudu ze dne 19.12.2013, sp. zn. 29 Cdo 1953/2013.

České časopisecké články

TOMÍŠEK, Jan. Právní jednání biometrickými prostředky v elektronickém bankovnictví. Právní rozhledy, 2018, č. 5, s. 160-167.

Seznam obrázků