UDK 347.952.2(497.4):336.777.7

Ukrepi za zagotavljanje varnosti pri plačevanju

*Anja Rijavec Uršej in Rebeka Reven**

MEASURES USED TO DELIVER PAYMENT SECURITY

The rise of digital payment methods and online shopping has driven the growing use of electronic payments, particularly innovative online solutions. However, advanced digital payment methods also introduce new risks, including fraud. Ensuring payment service providers lead in detecting and preventing fraud to offer secure payments is a complex challenge. The article examines current legislation, focusing on the Second Payment Services Directive (PSD2) and the European Commission's Delegated Regulation. It delves into the impact of PSD2, outlines prevalent fraud methods, and introduces the Verification of Payee (VoP), a security measure in this year's Instant Payments Regulation (IPR). Significant attention is given to proposed provisions on fraud within the upcoming Payment Services Regulation (PSR). The article also touches on non-binding recommendations and ongoing initiatives aimed at enhancing payment security.

JEL R30

1. Uvod

Razvoj digitalnih načinov plačevanja in rast spletnega nakupovanja sta pripomogla k vse večji uporabi elektronskih načinov plačevanja in zlasti inovativnih metod za spletno plačevanje. Poseben pospešek digitalnemu opravljanju finančnih storitev nasploh je dala epidemija covida-19, ki je zaradi želje opravljati storitve brez fizičnega stika do določene mere trajno spremenila navade uporabnikov. S tem je še dodatno okrepila postopen prehod na digitalna plačila ter potrdila ključen pomen varnih, dostopnih in priročnih plačil (vključno z brezstičnimi) za transakcije na daljavo in transakcije izvedene ob fizični prisotnosti plačnika (Evropska komisija, 2020).

Digitalizacija finančnih storitev lahko zaradi večje učinkovitosti (npr. nižji stroški in hitrejša izvršitev), večje priročnosti za uporabnike (npr. boljši distribucijski kanali in uporaba enostavnejših vmesnikov), izboljšanja finančne vključenosti, večje transparentnosti finančnih transakcij in hitrejšega odziva na (morebitne) krize (npr. zaradi hitrejše komunikacije in pomoči pri hitrejšem sprejemanju odločitev) prinese koristi tako gospodarstvu kot prispeva tudi k finančni stabilnosti (BIS, 2023). Vendar naprednejše plačilne rešitve prinašajo tudi nove oblike tveganj, med njimi tveganje goljufij: goljufi izrabljajo digitalizacijo za izvrševanje spletnih goljufij v vse večjem obsegu in v konstantno spreminjajočih se modalitetah – neobhodno je agilnost goljufov neprimerno večja kot odziv na spremembe pri ponudnikih plačilnih storitev pa tudi pri regulatorjih.

Ekosistem spletnih kriminalcev je vse bolj organiziran in omogoča celo, da šibkosti v verigi izvrševanja plačil izkoristijo tudi kriminalci brez tehničnega znanja in sposobnosti uporabe naprednih orodij, saj tovrstna orodja enostavno kupijo na črnem trgu (ang. Crime as a service). Ukradene in zlorabljene podatke o plačilnih karticah ter dostop do spletnega oziroma mobilnega bančništva nepazljivih uporabnikov plačilnih storitev namreč lahko kriminalci kupijo na za ta namen vzpostavljenih spletnih tržnicah na temnem spletu. Modalitete goljufij so tudi vedno bolj sofisticirane, zlonamerne kode so prilagojene različnim plačilnim kanalom oziroma instrumentom in zaobidejo varnostne ukrepe, kot je močna (dvofaktorska) avtentikacija strank.

Da bi uporabniki uporabljali elektronske načine plačevanja in tako izkoristili pozitivne učinke digitalizacije, je ključno zagotoviti in ohranjati zaupanje ne le uporabnikov plačilnih storitev, ampak uporabnikov finančnih storitev nasploh (EBA, 2023). In ob upoštevanju zgoraj navedenega imajo pri tem ključno vlogo ukrepi in orodja za preprečevanje goljufij pri plačilih. Prav zato je varnost plačilne infra-

* Anja Rijavec Uršej in Rebeka Reven, Banka Slovenije
Stališča, izražena v predstavitvi, niso nujno tudi stališča Banke Slovenije.

strukture v fokusu vizije Evropske komisije v zvezi z malimi plačili EU: »Cilj pravnega reda o malih plačilih je poskrbeti, da sta uporabnikom plačilnih storitev EU pri digitalnem plačevanju zagotovljeni preglednost in varnost.« (Evropska komisija, 2020).

Zaznana dinamika narave goljufij pri plačevanju ter sposobnost goljufov prilagajati se novim zahtevam, namenjenim preprečevanju goljufij, terjata drugačen, spremenjen pristop regulative (EBA, 2024). Vendar pa odgovor na vprašanje, kako zagotoviti, da bodo ponudniki plačilnih storitev prvi na področju odkrivanja in preprečevanja prevar ter bodo s tem svojim uporabnikom zagotovili zadostno varnost pri plačevanju, nikakor ni enostaven. V članku bova najprej opisali veljavno zakonodajo, torej 2. Direktivo o plačilnih storitvah[1] (PSD2) in njo dopolnjujočo delegirano uredbo Evropske komisije. Sledi vpogled v oceno učinka PSD2 in današnje modalitete goljufij ter opis dodatnega varnostnega ukrepa, to je ukrep preverjanja prejemnika plačila (ang. Verification of payee – VoP), ki ga določa v letošnjem letu sprejeta Uredba o takojšnjih plačilih[2] (IPR). Bistveni del članka je pregled predlaganih določb glede varnostnih ukrepov v novem pravnem okvirju za opravljanje plačilnih storitev – predvideno je namreč, da bosta PSD2 nadomestili nova Uredba o plačilnih storitvah in nova Direktiva o plačilnih storitvah, ki sta predmet razprave zakonodajnega postopka v Evropskem parlamentu in Svetu EU. Ker pa pravni okvir določa le bistvene in zahteve abstraktne narave, da jih lahko v svoje poslovanje vpeljejo vsi ponudniki plačilnih storitev v Evropski uniji, se v članku dotakneva tudi pregleda nezavezujočih priporočil in aktivnosti, ki potekajo za okrepitev varnosti pri plačevanju.

2. Veljavna zakonodaja

V Evropski uniji je digitalizacija plačil pospremljena z intervencijami regulatorjev, katerih cilj je izboljšanje učinkovitosti, varnosti in transparentnosti, vključno s poročanjem podatkov o goljufijah s strani ponudnikov plačilnih storitev (BIS, 2023).

Sistemsko ureditev opravljanja plačilnih storitev določa PSD2, ki so jo morale države članice v svoje nacionalne pravne rede prenesti v dveh letih po začetku njene veljave, to je do januarja 2018. PSD2 je v regulatorni okvir opravljanja plačilnih storitev prinesla nekaj pomembnih novosti, med njimi (strožje) zahteve glede varnosti pri plačilih in obvezne močne avtentikacije strank. Poleg tega je PSD2 z regulacijo dveh dodatnih plačilnih storitev, to sta storitev odobritve plačila in storitev zagotavljanja informacij o računih (storitvi t. i. odprtega bančništva), pripoznala širjenje ekosistema plačil ter, vsaj v primeru dveh novih plačilnih storitev, uredila obveznosti in pravice tudi za nove člene v plačilni verigi – tretje ponudnike storitev. Slednje je pomembno tudi z vidika zagotavljanja varnosti opravljanja teh dveh plačilnih storitev ter drugačne razdelitve odgovornosti v primeru, če pride do goljufij in izgube denarnih sredstev uporabnikov. PSD2 dopolnjujejo akti Evropskega bančnega organa (EBA) in delegirane uredbe Evropske komisije. Med njimi velja z vidika ukrepov za zagotavljanje varnosti pri plačevanju izpostaviti zlasti Delegirano uredbo Komisije (EU) 2018/389 glede regulativnih tehničnih standardov za močno avtentikacijo strank ter skupnih in varnih odprtih standardov komunikacije[3] (Delegirana uredba).

Kljub sistemski naravi PSD2 je pravna ureditev opravljanja plačilnih storitev čedalje večkrat dopolnjena z ločenimi, a vsebinsko povezanimi pravnimi akti. Primer je uredba SEPA Uredba[4], ki je bila nazadnje dopolnjena z IPR. Kot navedeno v uvodu je IPR uvedla ukrep preverjanja prejemnika plačila, ki bo moral biti po izteku prehodnega obdobja izveden pri vseh kreditnih plačilih (ne le pri takojšnjih).

Slovenija je PSD2 implementirala z Zakonom o plačilnih storitvah, storitvah izdajanja elektronskega denarja in plačilnih sistemih (ZPlaSSIED). Nacionalna ureditev sledi ureditvi v PSD2, saj ta uveljavlja načelo popolne harmonizacije, kar pomeni, da država članica ne sme zadevnega področja urediti drugače, kot ga ureja direktiva (razen v primeru, ko takšno možnost oziroma opcijo določi že sama direktiva) – zato v članku navajava ureditev v PSD2 in ne v ZPlaSSIED.

Pomembno pa je izpostaviti, da pravo EU, drugače kot to velja za zakonodajo, ki pripomore k delovanju enotnega trga (med to sodi tudi zakonodaja, ki ureja opravljanje plačilnih storitev), ne harmonizira tudi civilnega prava – ureditev tega je v rokah posameznih držav članic. Zato pravno ureditev opravljanja plačilnih storitev PSD2 (in posledično ZPlaSSIED) v Sloveniji dopolnjuje Obligacijski zakonik. Za vprašanja, ki niso urejena z ZPlaSSIED, se zato glede razmerja med ponudnikom plačilnih storitev in uporabnikom uporabljajo določbe Obligacijskega zakonika v zvezi s pogodbo o naročilu.

[1] Direktiva (EU) 2015/2366 Evropskega parlamenta in Sveta z dne 25. novembra 2015 o plačilnih storitvah na notranjem trgu, spremembah direktiv 2002/65/ES, 2009/110/ES ter 2013/36/EU in Uredbe (EU) št. 1093/2010 ter razveljavitvi Direktive 2007/64/ES

[2] Uredba (EU) 2024/886 Evropskega parlamenta in Sveta z dne 13. marca 2024 o spremembi uredb (EU) št. 260/2012 in (EU) 2021/1230 ter direktiv 98/26/ES in (EU) 2015/2366 glede takojšnjih kreditnih prenosov v eurih

[3] Delegirana uredba Komisije (EU) 2018/389 z dne 27. novembra 2017 o dopolnitvi Direktive (EU) 2015/2366 Evropskega parlamenta in Sveta glede regulativnih tehničnih standardov za močno avtentikacijo strank ter skupnih in varnih odprtih standardov komunikacije

[4] Uredba (EU) 2021/1230 Evropskega parlamenta in Sveta z dne 14. julija 2021 o čezmejnih plačilih v Uniji

2.1 PSD2 in Delegirana uredba

Čedalje večja kompleksnost elektronskih plačil – pa čeprav so ta za uporabnike zaradi prizadevanj ponudnikov za dobro uporabniško izkušnjo enostavna za uporabo, vedno bolj pa zaradi vpetosti v postopek nakupa za plačnika celo nezaznavna – ter obseg le-teh na globalni ravni in novi načini plačevanja prinašajo tudi nova varnostna tveganja. Varnost pa je bistveni pogoj za dobro delujoč trg plačilnih storitev, zato morajo biti njihovi uporabniki ustrezno zaščiteni. To je razlog, da je zakonodajalec EU v PSD2 bistveno bolj kot v predhodno direktivo PSD1 vključil zahteve za izvajanje varnostnih ukrepov, potrjevanja plačilnih transakcij in rednega poročanja. Po drugi strani pa so kljub čedalje večji kompleksnosti ekosistema plačil obveznosti in pravice ter odgovornost, če (ko) do goljufij pride, v PSD2 porazdeljene le med stranke pogodbe o opravljanju plačilnih storitev, torej ponudnike in uporabnike plačilnih storitev.

Bistvena novost na področju varnosti plačil, ki jo je prinesla PSD2, je zahteva, da morajo vsi ponudniki plačilnih storitev uporabljati močno avtentikacijo strank, ki vsebuje elemente za dinamično povezavo transakcije z določenim zneskom in določenim prejemnikom plačila, vsakič, ko uporabnik izvede elektronsko plačilo ali dostopa do svojega vmesnika spletne banke oziroma opravi kakršno koli dejavnost prek kanala na daljavo, ki lahko pomeni tveganje plačilne goljufije ali drugih zlorab: uporabiti morajo avtentikacijske rešitve, ki temeljijo na uporabi dveh ali več elementov, ki so kategorizirani kot „znanje" (nekaj, kar ve samo uporabnik), „imetje" (nekaj, kar ima le uporabnik) in „inherenca" (nekaj, kar uporabnik je, npr. biometrija). Zaradi zagotovitve učinkovitosti močne avtentikacije strank je tudi ključno, da imajo ponudniki plačilnih storitev ustrezne varnostne ukrepe, s katerimi zavarujejo zaupnost in celovitost osebnih varnostnih elementov uporabnikov plačilnih storitev (97. člen PSD2). Če plačnikov ponudnik plačilnih storitev ne zahteva močne avtentikacije strank, plačnik nosi finančne posledice morebitne goljufije le, če je ravnal goljufivo. Če prejemnikov ponudnik plačilnih storitev zavrne močno avtentikacijo stranke, mora v primeru goljufije povrniti finančno škodo povzročeno plačnikovemu ponudniku plačilnih storitev (92. člen PSD2).

Za učinkovito preprečevanje goljufij ter boj proti njim s preiskovanjem in odkrivanjem je PSD2 določila tudi pravno podlago za zbiranje, obdelavo in izmenjavo osebnih podatkov. Vendar pa ponudniki plačilnih storitev lahko dostopajo le do tistih osebnih podatkov, ki so potrebni za opravljanje njihovih plačilnih storitev, ter jih obdelujejo in hranijo z izrecnim soglasjem uporabnika plačilnih storitev (94. člen PSD2). V primeru zaznave suma, da gre za neodobreno ali goljufivo uporabo plačilnega instrumenta, in če je tako določeno v okvirni pogodbi (oziroma splošnih pogojih kot del te), lahko ponudniki plačilnih storitev v skladu z 68. členom PSD2 blokirajo plačilni instrument ter o blokadi in razlogih zanjo obvestijo uporabnike.

Goljufij ne morejo preprečiti oziroma, če se te zgodijo, minimizirati njihovih učinkov zgolj ponudniki plačilnih storitev. Uporabniki plačilnih storitev morajo plačilni instrument uporabljati v skladu s pogoji, ki urejajo izdajo in uporabo plačilnega instrumenta, ter brez nepotrebnega odlašanja obvestiti ponudnike plačilnih storitev ali subjekte, ki jih ti določijo, če ugotovijo, da je bil plačilni instrument izgubljen, ukraden, zlorabljen ali uporabljen brez dovoljenja (69. člen PSD2), ter tako zmanjšati tveganje neodobrenih plačilnih transakcij. Prvi pogoj za to je seveda, da ponudniki plačilnih storitev izpolnijo svojo obveznost glede vzpostavitve kanala za posredovanja informacij.

PSD2 je določbe o odgovornosti za izvršitev neodobrenih transakcij določila na način, da zaradi preprečevanja moralnega hazarda obeh pogodbenih strank izgube razporeja med ponudnike in uporabnike plačilnih storitev. Ker je oblikovanje plačilnih produktov, opravljanje plačilnih storitev ter izbira pogodbenih izvajalcev tehničnih storitev v rokah ponudnikov plačilnih storitev, je tudi odgovornost za povrnitev denarnih sredstev v primeru realizacije neodobrenih plačilnih transakcij primarno na ponudnikih: v primeru neodobrenih plačilnih transakcij bi bilo treba plačniku nemudoma povrniti znesek zadevne transakcije (71. uvodna izjava PSD2). Ponudniki plačilnih storitev lahko v skladu s 74. členom PSD2 potrošnika[5] s pogodbo zavežejo k participaciji pri kritju izgub zaradi izgube ali kraje plačilnega instrumenta ali njegove zlorabe v višini do največ 50 EUR, razen če je ravnal goljufivo ali hudo malomarno. Vendar pa ponudniki plačilnih storitev ne smejo določiti participacije plačnikov pri izgubi, če (i) izgube, kraje ali zlorabe plačilnega instrumenta ni bilo mogoče odkriti pred izvedbo plačila, razen če so plačniki sami ravnali goljufivo; ali je (ii) izguba posledica dejanj ali neukrepanja zaposlenih, zastopnikov ali podružnic ponudnikov plačilnih storitev ali zunanjih izvajalcev. Plačniki tudi ne smejo nositi nobenih finančnih posledic uporabe izgubljenega, ukradenega ali zlorabljenega plačilnega instrumenta po tem, ko so o tem obvestili svojega ponudnika plačilnih storitev. Po drugi strani pa uporabniki (plačniki) nosijo celotno izgubo v zvezi z neodobrenimi plačilnimi transakcijami, če so te posledica njihovega goljufivega ravnanja ali naklepno ali iz hude

[5] Za uporabnike plačilnih storitev, ki niso potrošniki, je zakonodajalec predvidel, da so taki uporabniki običajno zmožni bolje presoditi tveganje goljufije in sprejeti izravnalne ukrepe, zato omejitev participacije na 50 EUR zanje ne velja.

malomarnosti niso izpolnile ene ali več obveznosti, ki jim jih nalaga PSD2 (pri čemer lahko države članice z nacionalno zakonodajo to odgovornost uporabnikov ob upoštevanju značilnosti osebnih varnostnih elementov in posebnih okoliščin tudi znižajo – te opcije Slovenija pri implementaciji PSD2 ni uporabila).
Zgoraj opisana razdelitev odgovornosti PSD2 za izgubo denarnih sredstev, ko do goljufije pride, je precej natančno urejena, običajno pa se zatakne pri presoji, ali je bila plačilna transakcija odobrena (ali ne) ter ali je prišlo do neodobrene plačilne transakcije zaradi hudo malomarnega ravnanja uporabnika. Pri ocenjevanju morebitne malomarnosti uporabnika nas 72. uvodna izjava PSD2 napotuje na upoštevanje vseh okoliščin konkretnega primera ter nacionalno zakonodajo. Pogodbeni pogoji v zvezi z zagotavljanjem in uporabo plačilnega instrumenta, ki bi posledično povečali dokazno breme za potrošnike ali zmanjšali dokazno breme za izdajatelje, bi se v skladu z 72. uvodno izjavo PSD2 morali šteti za nične in neveljavne. Slovenska sodna praksa abstrakten pravni pojem hude malomarnosti napolnjuje z opredelitvijo, da se »vprašanje hude malomarnosti ne presoja samo glede pričakovanega ravnanja normalno skrbnega uporabnika, ampak tudi manj skrbnega uporabnika«[6]. Poleg tega 72. uvodna izjava PSD2 v posebnih razmerah, zlasti če plačilni instrument ni prisoten na prodajnem mestu, kot v primeru spletnih plačil prek interneta, kot primerno ocenjuje, da morajo ponudniki plačilnih storitev zagotoviti dokaz domnevne [hude] malomarnosti, saj imajo plačniki v takih primerih zelo omejene možnosti, da to storijo.
Ureditev PSD2 dopolnjuje Delegirana uredba, ki temelji na osnutkih regulativnih tehničnih standardov, ki jih je Evropski komisiji predložila EBA. V vseh državah članicah neposredno veljavna Delegirana uredba poleg skupnih in varnih standardov komunikacije v povezavi z določbami PSD2 glede odprtega bančništva določa zahteve, ki jih morajo izpolnjevati ponudniki plačilnih storitev za izvajanje ukrepov za zagotavljanje varnosti pri plačilih. Delegirana uredba tako natančneje določa uporabo postopka močne avtentikacije strank v skladu s PSD2 ter zaščite zaupnosti in celovitosti osebnih varnostnih elementov uporabnikov plačilnih storitev.
Določbe Delegirane uredbe pri dopolnitvi PSD2 krmarijo med varnostjo in na drugi strani možnostjo zagotavljanja dobre uporabniške izkušnje ob upoštevanju specifične narave pomembnih okoliščin za varnost plačil (9. uvodna izjava Delegirane uredbe). Zato je delegirana uredba določila izjeme od uporabe močne avtentikacije strank, za katere veljajo določeni in omejeni pogoji na podlagi stopnje tveganja, zneska in ponovitev plačilne transakcije ter plačilnih kanalov, ki se uporabljajo za izvršitev plačilnih transakcij. Izjeme se nanašajo na:

- vpogled v informacije o plačilnih računih brez razkritja občutljivih podatkov o plačniku,
- brezstična plačila na prodajnih mestih,
- plačila na samopostrežnih terminalih za javni prevoz in parkirnine,
- plačilne transakcije preverjenim prejemnikom plačil,
- ponavljajoča se plačila,
- kreditna plačila med računi iste fizične ali pravne osebe,
- plačilne transakcije majhnih vrednosti (do 30 evrov),
- plačilne transakcije pravne osebe, ki uporablja varne plačilne postopke in protokole,
- plačilne transakcije, pri katerih analiza tveganja pokaže, da predstavljajo nizko stopnjo tveganja (pogoje za tako določitev določa Delegirana uredba).

Delegirana uredba je ponudnikom plačilnih storitev določila tudi pravno zahtevo vzpostavitve mehanizmov za spremljanje (monitoring) transakcij, ki jim omogočajo zaznavanje neodobrenih oziroma goljufivih plačilnih transakcij ter posledično nadaljnje varnostne ukrepe. Navedeni mehanizmi temeljijo na analizi plačilnih transakcij ob upoštevanju elementov, ki so tipični za (konkretnega) uporabnika plačilnih storitev v okoliščinah običajne uporabe osebnih varnostnih elementov.

2.2 Učinek PSD2 in predlogi EBA za spremembo zakonodaje

Tako Evropska centralna banka (Evropska centralna banka, 2023) kot EBA (EBA, 2022) sta na podlagi podatkov, ki so jih poročali ponudniki, ocenili, da je bila močna avtentikacija strank skupaj z zahtevo po spremljanju (monitoringu) plačilnih transakcij in drugimi varnostnimi ukrepi PSD2 in Delegirane uredbe v celoti uspešna pri upravljanju s tveganjem goljufij (EBA, 2024). Število goljufij pri kartičnih plačilnih transakcijah odrejenih na daljavo je bilo namreč kar petkrat nižje pri plačilnih transakcijah z izvedeno močno avtentikacijo strank v primerjavi s plačilnimi transakcijami, pri katerih močna avtentikacija strank ni bila izvedena, ter trikrat nižje glede na podatke o vrednosti goljufij pri plačilnih transakcijah (EBA, 2022). V letu 2022 se je glede na poročanje plačnikovih ponudnikov plačilnih storitev močna avtentikacija strank uporabila pri 70 odstotkih kreditnih plačil odrejenih na daljavo in pri 36 odstotkih kartičnih transakcij, odrejenih na daljavo. Uporaba izjem od izvedbe močne avtentikacije v

[6] VSRS Sodba III Ips 62/2019 z dne 11. 5. 2020, ki je odločila tudi, da »od manj skrbnega uporabnika spletne banke gotovo ni pričakovati, da bo pozorno prebral in upošteval vsak stavek v obvestilih, ki mu jih banka pošlje, še posebej, ker teh obvestil ni malo.«.

skladu z Delegirano uredbo je bila posledično zlasti zabeležena pri teh dveh plačilnih kanalih (EBA, 2024). Kljub zelo ugodnemu vplivu močne avtentikacije strank na zniževanje goljufij pri plačilih je EBA zaznala višje tveganje za goljufije pri nekaterih specifičnih plačilnih instrumentih. EBA je zlasti izpostavila takojšnja kreditna plačila, pri katerih je stopnja zlorab v povprečju EU 10-krat večja kot pri navadnih kreditnih plačilih (podatki po državah članicah se sicer precej razlikujejo). Razlog za to bi lahko bil v bistveno težjem sledenju in zaustavitvi tovrstnih plačilnih transakcij zaradi tehničnih ovir. Nadalje je tveganje za goljufije povezano z geografskimi dimenzijami in/ali jurisdikcijami, saj so goljufije bistveno višje pri čezmejnih transakcijah kot pri domačih – analiza EBA kaže, da kar za 9-krat tako pri kartičnih kot pri kreditnih plačilih. EBA nenazadnje opozarja na porazdelitev izgub iz naslova goljufij med ponudniki in uporabniki plačilnih storitev kot tudi drugimi subjekti v verigi plačil, ki bistveno variirajo glede na vrsto plačilnega instrumenta. V letu 2022 so bile tako izgube zaradi goljufij pri kartičnih transakcijah relativno enakomerno razdeljene med ponudnike (in druge subjekte udeležene v verigi plačil na strani ponudbe) in uporabnike, po drugi strani pa so kar 79 % oziroma za 1,2 milijardi evrov izgub zaradi goljufij pri kreditnih plačilih nosili uporabniki (EBA, 2024).
Za nadaljnje zniževanje goljufivih plačilnih transakcij je po mnenju EBA treba ureditev PSD2 in Delegirane uredbe razširiti na nekatere specifične zahteve za kartične sheme, plačilne vmesnike (ang. Payment Gateways) in prodajna mesta v plačilnih situacijah, v katerih imajo ti subjekti pomembno vlogo. Nadalje je EBA priporočila podrobnejšo razdelitev odgovornosti za povrnitev denarnih sredstev, ki so predmet goljufij, med tretjimi ponudniki plačilnih storitev in ponudniki, ki vodijo plačilni račun uporabnika, ter med izdajatelji in pridobitelji plačilnih instrumentov, kadar je bila uporabljena izjema od močne avtentikacije v skladu z Delegirano uredbo. Prav tako je po mnenju EBA treba konkretneje opredeliti ključne pojme z vidika preprečevanja prevar v PSD2 (utemeljeni sumi na goljufijo, dejanje goljufije, velika malomarnost in druge), saj je njihova abstraktnost vodila v pravno negotovost, nekonsistentno uporabo PSD2 ter predstavlja izziv pristojnim nacionalnim nadzornim organom pri presoji odgovornosti nadzorovanih subjektov za neodobrene plačilne transakcije. Nadalje je EBA glede same močne avtentikacije strank na Evropsko komisije naslovila predlog, naj razjasni, ali naj bo uporaba izjem po Delegirani uredbi opcijska ali obvezna ter da naj se jasno določi, da je močna avtentikacija strank preventivni in korekcijski ukrep in bi kot tak moral biti (za uporabnike) brez doplačil.

Nadalje je EBA na Evropsko komisijo naslovila še številne druge predloge sprememb glede močne avtentikacije strank, med njimi glede upravljanja tveganja goljufij s socialnim inženiringom ter nujne skrbi za določene družbene skupine, da zaradi načina izvajanja močne avtentikacije strank s strani ponudnikov plačilnih storitev ne bodo de facto izključene iz uporabe plačilnih storitev kot fundamentalne vrste finančnih storitev (EBA, 2022).

3. Pojavnost goljufij po uveljavitvi PSD2

Evropska centralna banka in EBA sta na podlagi poročanja ponudnikov plačilnih storitev ocenila, da je bila škoda zaradi goljufij pri plačilih v letu 2022 4,3 milijarde EUR, v prvi polovici leta 2023 pa 2,0 milijarde EUR. Glede na poročilo je večina goljufij povezanih s kartičnimi in kreditnimi plačili. Slednja izstopajo tudi relativno, goljufivih je bilo namreč 0,031 % vseh kartičnih plačil po vrednosti in 0,015 % vseh kartičnih plačil po številu transakcij. Po drugi strani je bilo več kot polovica goljufij, povezanih s kreditnimi plačili, povezanih z manipulacijo plačnika, da je odredil plačilni nalog (Evropska centralna banka, 2023). V zvezi z novimi tipologijami prevar je EBA pričakovano opazila, da so se goljufi začeli prilagajati spremenjenim tehnološkim in regulatornim okoliščinam: ker je močna avtentikacija strank učinkovita pri preprečevanju goljufij, ki so posledica kraje uporabnikovih varnostnih elementov, so se po uveljavitvi PSD2 pojavili novi ali razširili obstoječi tipi goljufij bolj kompleksne narave. Te lahko uvrstimo v eno od treh kategorij:

- manipulacija uporabnika s socialnim inženiringom, da opravi plačilno transakcijo – ta način goljufije je relativno neodvisen od tehničnih varnostnih ukrepov ponudnikov plačilnih storitev in običajno temelji na zbranih podatkih o konkretnem uporabniku, na primer prek socialnih omrežij, velikokrat s predstavljanjem kot uporabniku poznane in zaupanja vredne osebe (kot so sorodniki, prijatelji, poslovni partnerji, davčni organ ali uporabnikov ponudnik plačilnih storitev);
- goljufije s kombinacijo socialnega inženiringa in tehnične goljufije, pri kateri goljufi kombinirajo različne oblike ribarjenja (ang. phishing), vključno s tehnikama vishinga in smishinga, za krajo uporabnikovih osebnih varnostnih elementov za prevzem nadzora nad uporabnikovim plačilnim računom in odrejanje plačilnih nalogov ter s socialnim inženiringom, ki cilja na uporabnikovo avtorizacijo plačilnih nalogov;
- vdor v postopek vpisa uporabnika v spletno ali mobilno banko, ki cilja na vpis goljufov v napravo kot drugega faktorja močne avtentikacije uporabnika z uporabo ukradenih osebnih varnostnih elementov uporabnika

(s fishingom, smishingom ali vishingom). Te vrste goljufij velikokrat izkoristijo specifične šibkosti postopka vpisa v spletno ali mobilno banko, ki goljufom povsem omogočijo nadzor nad plačilnim računom uporabnika, kar izkoristijo za serijo goljufivih plačilnih transakcij (EBA, 2024).

Za Slovenijo izpostavlja SI-CERT glede na podatke za prvo polovico leta 2024 goljufije, izvedene prek mobilnih telefonov, ter trend pripisuje t. i. ang. mobile first konceptu, to je konceptu zasnove spletnih aplikacij, ki pred drugimi vidiki upoštevajo uporabniško izkušnjo na mobilnih napravah. Kot primer izpostavlja lažna SMS-sporočila (smishing) v imenu bank in dostavnih služb, s katerimi želijo goljufi priti do podatkov mobilne denarnice ali kreditne kartice. Ter nadalje, da »skušajo žrtve doseči tudi z uporabo aplikacij, kjer želijo žrtev zvabiti v kriptoinvesticijsko ali ljubezensko prevaro.« (SI-CERT, 2024). SI-CERT je v letu 2023 obravnaval 216 primerov tovrstnih smishing prevar, kar predstavlja skoraj petkratno povečanje v primerjavi s predhodnim letom. Policija tudi v letu 2024 beleži porast prijav goljufij na spletu za okrog 30 %. V letu 2023 je sicer obravnavala okrog 1700 prijav spletnih goljufij, pri čemer je bila skupna nastala škoda okrog 27,5 milijona evrov, v letu 2024 pa so do sredine oktobra prejeli okrog 1600 prijav s skupno škodo 25,5 milijona evrov. Najpogostejše prijave goljufij na spletu, ki jih prejme policija, so prevare z nikoli dostavljenimi artikli. Sledijo investicijske goljufije, pri katerih goljuf pokliče po telefonu ter kot pogoj za izplačilo teh sredstev navede namestitev programa za oddaljen dostop (na primer aplikacije z imeni Anydesk in Supremo) na računalnik ali mobilno napravo, zaradi česar lahko goljufi s to aplikacijo vstopijo v spletno oziroma mobilno banko in odtujijo vsa denarna sredstva na plačilnem računu oškodovanca (ZBS, 2024).

4. Ukrep preverjanja prejemnika plačila

Kot navedeno zgoraj je EBA zaradi specifične narave takojšnjih kreditnih plačil[7] in višanja tveganja goljufij pri kreditnih plačilih nasploh so-zakonodajalcema EU priporočila uvedbo ustreznih ukrepov za preprečevanje tveganj goljufij (EBA, 2022). Varnostna tveganja so še zlasti relevantna v luči pričakovanega učinka Uredbe o takojšnjih plačilih (IPR), ki ponudnikom plačilnih storitev, ki ponujajo (navadna) takojšnja plačila, nalaga, da v letu 2025 svojim uporabnikom zagotovijo tudi prejemanje in pošiljanje takojšnjih plačil.
Z IPR je zato uveden ukrep t. i. preverjanja prejemnika plačnika, v predlogu Evropske komisije sprva le pri takojšnjih kreditnih plačilih, so-zakonodajalca EU pa sta nato zahtevo po izvajanju IBAN z nazivom prejemnika plačila z notifikacijo plačnika o stopnji ujemanja pri izvajanju vseh kreditnih prenosov od 9. oktobra 2025 razširila na vsa kreditna plačila. S tem bodo preprečevali, da bi uporabniki plačilnih storitev (plačniki) ali kot žrtve goljufij (zlasti socialnega inženiringa) ali zaradi napake pri vpisu podatkov poslali plačilo nenamernemu prejemniku plačila, ki ga naknadno ne bi mogli izterjati nazaj. Ponudniki plačilnih storitev plačnikov bodo morali preverjanje prejemnika plačila opraviti takoj potem, ko bodo plačniki posredovali ustrezne informacije o prejemnikih plačil in preden se bodo plačnikom ponudile možnosti odobritve navedenega kreditnega prenosa (5.c člen IPR).

5. Zakonodaja v nastajanju: predlog Uredbe o plačilnih storitvah na notranjem trgu (PSR)

Evropska komisija je 28. junija 2023 objavila predlog revizije PSD2, v obliki predloga Uredbe o plačilnih storitvah na notranjem trgu (PSR)[8], ki vključuje pravila za ponudnike plačilnih storitev in potrošnike, ter predloga Direktive o plačilnih storitvah in storitvah elektronskega denarja na notranjem trgu (PSD3),[9] ki zajema zlasti pravila o izdajanju dovoljenj plačilnim institucijam in nadzoru nad njimi. Cilj predloga revizije PSD2 je evolucija in ne revolucija, preprečevanje zlorab pa je zaradi pomembnosti za učinkovit trg plačil in zaupanja uporabnikov v varnost plačil v fokusu predloga PSR.
Osnova za to poglavje je besedilo predloga PSR, ki ga je objavila Evropska komisija junija lansko leto, poudariti pa je treba, da določbe še niso dokončne. Predlog PSR je namreč trenutno predmet obravnave v zakonodajnem postopku EU, konkretneje pri so-zakonodajalcih EU, tj. v Evropskem parlamentu in v Svetu EU. Časovnica obravnave predlogov do sprejema je negotova oziroma se predvidenega zaključka pogajanj v zakonodajnih telesih ne da napovedati.
Boj proti goljufijam pri plačilih se s predlogom PSR vzpostavlja v vseh korakih plačilne verige. Zajema dodatne ukrepe za preprečevaje in omejevanje goljufij, ki jih lahko razdelimo v štiri vsebinske sklope:

1. ozaveščanje uporabnikov plačilnih storitev, zlasti potrošnikov,
2. spremljanje plačilnih transakcij v realnem času in drugi s tem povezani ukrepi ponudnikov plačilnih storitev,

[7] Takojšnja kreditna plačila so kreditna plačila, ki se izvedejo v 10 sekundah.

[8] Predlog Uredbe Evropskega parlamenta in Sveta o plačilnih storitvah na notranjem trgu in dopolnitvi Uredbe (EU) št. 1093/2010.

[9] Predlog Direktive Evropskega parlamenta in Sveta o plačilnih storitvah in storitvah elektronskega denarja na notranjem trgu, spremembi Direktive 98/26/ES ter razveljavitvi direktiv (EU) 2015/2366 in 2009/110/ES.

3. vzpostavitev pravne podlage za izmenjavo podatkov ter
4. skrb za žrtve goljufij, če se goljufija zgodi.

5.1 Ozaveščanje uporabnikov plačilnih storitev, zlasti potrošnikov

Goljufi uporabljajo manipulativne tehnike in tehnike izdajanja za drugo osebo, s čimer postajajo plačilne goljufije vse bolj dodelane in prefinjene. Zaradi tega jih uporabniki plačilnih storitev težko prepoznajo brez ustrezne ozaveščenosti in informiranosti. V takih primerih lahko ponudniki plačilnih storitev igrajo ključno vlogo ter pomembno prispevajo k preprečevanju goljufij, če redno ozaveščajo uporabnike plačilnih storitev o tveganjih in novih trendih plačilnih goljufij (106. uvodna izjava predloga PSR).

Iz predloga PSR izhaja, da bodo morali ponudniki plačilnih storitev izvajati aktivnosti ozaveščanja tako za svoje stranke kot tudi za svoje zaposlene. Za svoje stranke (uporabnike plačilnih storitev) bodo morali pripraviti ustrezne programe in kampanje za ozaveščanje o trendih in tveganjih goljufij. Uporabnikom bodo morali prek različnih medijev posredovati informacije o goljufijah in pojavu novih oblik goljufij. Pripraviti bodo morali jasna sporočila in opozorila, v katerih jim bodo morali pojasniti, (i) kako prepoznati poskuse goljufij, (ii) kakšne varnostne ukrepe morajo upoštevati, da ne bi postali žrtev goljufij, ter nenazadnje, (iii) kje goljufije prijaviti. Za svoje zaposlene bodo morali ponudniki plačilnih storitev vsaj enkrat letno organizirati programe usposabljanja o tveganjih in trendih plačilnih goljufij. S tem bodo zagotovili, da so njihovi zaposleni ustrezno usposobljeni za opravljanje svojih nalog in odgovornosti (84. člen predloga PSR).

EBA pa bo morala, kot izhaja iz predloga PSR, pripraviti smernice o različnih vrstah programov o tveganjih in trendih plačilnih goljufij, ki jih bodo morali za svoje stranke in zaposlene izvajati ponudniki plačilnih storitev glede na nenehno spreminjajočo se naravo tveganj, povezanih z goljufijami (84. člen predloga PSR).

5.2 Spremljanje plačilnih transakcij v realnem času in drugi s tem povezani ukrepi ponudnikov plačilnih storitev

5.2.1 Mehanizmi za spremljanje transakcij

Za učinkovito preprečevanje goljufivih transakcij je ključno njihovo pravočasno odkrivanje, kar omogočajo mehanizmi za spremljanje transakcij. Ponudnike plačilnih storitev k temu sicer zavezuje že Delegirana uredba, kot je pojasnjeno v poglavju 2.1., zdaj pa se bo to preneslo in dodatno uredilo v predlogu PSR. Predlog PSR namreč od ponudnikov plačilnih storitev zahteva vzpostavitev mehanizmov za spremljanje transakcij, ki omogočajo uporabo močne avtentikacije strank, ter boljše preprečevanje in odkrivanje goljufivih transakcij. Ti mehanizmi bodo pokazali njihov ključni prispevek k preprečevanju goljufij in presegali zaščito, ki jo zagotavlja močna avtentikacija strank (100. uvodna izjava predloga PSR).

Mehanizmi za spremljanje transakcij bodo morali temeljiti na analizi preteklih plačilnih transakcij. Upoštevati bodo morali značilnosti uporabnika plačilnih storitev v okoliščinah običajne uporabe osebnih varnostnih elementov. Iz obrazložitvenega memoranduma k predlogu PSR izhaja, da so takšne okoljske in vedenjske značilnosti na primer: (i) lokacija uporabnika plačilnih storitev, (ii) čas plačilne transakcije, (iii) uporabljena naprava, (iv) navade v zvezi z porabo ter (v) spletna trgovina, kjer je bil opravljen nakup. Na ta način se lahko odkrije netipično uporabo plačilnih storitev, ki nakazuje na morebitno goljufivo transakcijo.

Za učinkovito spremljanje transakcij, ki ponudnikom plačilnih storitev omogoča zaznavanje in preprečevanje goljufij, bodo morali imeti ponudniki možnost obdelave informacij o transakcijah in plačilnih računih svojih strank. Ob tem bodo morali ponudniki plačilnih storitev določiti ustrezna obdobja hrambe različnih vrst podatkov, namenjenih preprečevanju goljufij, ki bi morala biti strogo omejena na čas, potreben za zaznavanje netipičnih ali potencialno goljufivih dejanj (102. uvodna izjava predloga PSR).

Iz predloga PSR izhaja tudi to, da bo morala EBA pripraviti osnutek regulativnih tehničnih standardov o posebnih tehničnih zahtevah v zvezi z mehanizmi za spremljanje transakcij. Pomembno je, da bodo te zahteve morale temeljile na dodani vrednosti, ki izhaja iz okoljskih in vedenjskih značilnosti, povezanih s plačilnimi navadami uporabnika plačilnih storitev (101. uvodna izjava predloga PSR).

5.2.2 Izboljšave pri uporabi močne avtentikacije strank

V predlogu PSR so dodane določbe za izboljšanje dostopnosti močne avtentikacije strank, zlasti za zagotovitev, da bodo imeli vsi, vključno z invalidi, starejšimi osebami, osebami z nizko ravnjo digitalnih spretnosti in tistimi, ki nimajo dostopa do digitalnih kanalov, na voljo vsaj eno sredstvo, ki jim bo omogočalo izvedbo močne avtentikacije strank. To konkretno pomeni, da ponudniki plačilnih storitev izvedbe močne avtentikacije strank ne bodo smeli neposredno ali posredno pogojevati z uporabo pametnega telefona (88. člena predloga PSR).

Nadalje so zato, ker so se pojavile težave pri izvedbe močne avtentikacije strank v praksi, v predlog PSR vključili odgovornost ponudnikov tehničnih storitev in upravljavcev plačilnih shem. Iz 120. uvodne izjave predloga PSR izhaja,

da bi glede na vlogo, ki jo imajo pri zagotavljanju pravilnega izvajanja ključnih varnostnih zahtev v zvezi s plačili malih vrednosti, vključno z zagotavljanjem ustreznih rešitev s področja informacijske tehnologije, morali biti ponudniki tehničnih storitev in upravljavci plačilnih shem odgovorni za finančno škodo povzročeno prejemnikom plačila ali ponudnikom plačilnih storitev prejemnikov plačila ali plačnikov, če ne podpirajo uporabe močne avtentikacije strank (120. uvodna izjava predloga PSR).
Iz 58. člena predloga PSR izhaja, da bi bili ponudniki tehničnih storitev in upravljavci plačilnih shem, ki opravljajo storitve za prejemnika plačila ali za ponudnika plačilnih storitev prejemnika plačila ali plačnika, odgovorni za vso finančno škodo, ki bi jo utrpeli prejemnik plačila, ponudnik plačilnih storitev prejemnika plačila ali plačnikov ponudnik plačilnih storitev, ker v obsegu svojega pogodbenega razmerja niso opravili storitev, potrebnih da se omogoči uporaba močne avtentikacije strank.

5.2.3 Preverjanje prejemnika plačila

V okvir preventivnih ukrepov je uvrščena tudi obveznost preverjanja prejemnika plačila pri izvajanju vseh kreditnih prenosov, kar je medtem uredila že IPR. O tem sva podrobneje pisali v poglavju 4, preverjanje prejemnika plačila pri vseh kreditnih plačilih je bilo v (predlog) IPR dodano po objavi predloga PSR s strani Evropske komisije junija 2023.

5.3 Pravna podlaga za izmenjavo podatkov

Pogosto posamezni ponudnik plačilnih storitev nima celovitega vpogleda v vse dejavnike, ki bi lahko omogočili pravočasno odkrivanje goljufij. Pri tem bi bila večja učinkovitost odkrivanja mogoča s širšim naborom informacij o potencialno goljufivih aktivnostih, ki jih imajo tudi drugi ponudniki plačilnih storitev. Zaradi tega bi bilo, kot izhaja iz 103. uvodne izjave predloga PSR, priporočljivo omogočiti izmenjavo pomembnih podatkov med različnimi ponudniki plačilnih storitev.
Predlog PSR torej predvideva vzpostavitev pravne podlage za izmenjavo vseh pomembnih informacij o goljufivih transakcijah med ponudniki plačilnih storitev. Za ta namen bodo ponudniki plačilnih storitev sklenili dogovore o izmenjavi informacij, v katerih bodo opredelili tehnične in organizacijske ukrepe za varstvo osebnih podatkov.
Pred sklenitvijo dogovora o izmenjavi informacij bi morali ponudniki plačilnih storitev izvesti oceno učinka z varstvom podatkov skladno s 35. členom Uredbe o varstvu podatkov (GDPR)[10]. Če bi ta ocena pokazala, da bi obdelava brez zaščitnih in varnostnih ukrepov predstavljala visoko tveganje za pravice in svoboščine posameznikov, bi se morali posvetovati z ustreznim organom za varstvo podatkov skladno s 36. členom GDPR (83. člen predloga PSR). Podatke, ki bi se izmenjevali na podlagi večstranskega dogovora, bodo ponudniki plačilnih storitev lahko uporabljali izključno za izboljšanje mehanizma spremljanja transakcij.
Izmenjava informacij bo potekala na večstranski podlagi, na primer prek namenskih platform informacijske tehnologije. Ponudniki plačilnih storitev se bodo tako lahko zanesli na najbolj celovite in posodobljene informacije, in sicer s skupno uporabo informacij o enoličnih identifikacijskih oznakah, tehnikah manipulacije in drugih okoliščinah povezanih z goljufivimi transakcijami (103. uvodna izjava predloga PSR).
Da izmenjava informacij o sumljivih goljufivih dejavnostih ne bi privedla do neupravičenega zmanjševanja tveganja ali ukinitve plačilnih storitev uporabnikom brez jasnega pojasnila, bi morali ponudniki plačilnih storitev sprejeti določene zaščitne ukrepe. Prvi primer je vzpostavitev stika s stranko, če je ta plačnik potencialno goljufivega plačila. Drugi primer pa je nadaljnje spremljanje računa, če je stranka označena z enolično identifikacijsko oznako, ki jo drugi ponudniki plačilnih storitev prepoznajo kot potencialno goljufivo (105. uvodna izjava predloga PSR).

5.4 Skrb za žrtve goljufij, ko se goljufija že zgodi

Kljub vsem predhodno naštetim preventivnim ukrepom pa je nujno pozornost nameniti tudi kurativnim ukrepom, torej skrbi za žrtve goljufije. Iz predloga PSR izhaja, da se bo uredilo tudi situacije, ko so potrošniki plačilne transakcije odobrili, ker so bili žrtve goljufij. Zavedeni potrošniki namreč lahko odobrijo transakcijo, ki je dejansko niso želeli in so jo odobrili, ne da bi vedeli, da je transakcija goljufiva. Takšne goljufije so primeri (i) socialnega inženiringa, pri katerih se goljufi pretvarjajo, da so zaposleni pri ponudniku plačilnih storitev stranke, ter zlorabljajo njegovo ime, elektronski naslov ali telefonsko številko, ter primeri (ii) ko goljufi z zvijačo prevzamejo nadzor nad celotnim postopkom odobritve, vključno z dokončanjem močne avtentikacije strank, v celoti brez vednosti uporabnika. Te relativno nove vrste goljufij so zabrisale razliko, ki v PSD2 obstaja med odobrenimi in neodobrenimi transakcijami. Integriteta odobritve plačilne transakcije ja prav zaradi omenjenih manipulativnih tehnik goljufov vprašljiva, zato povračil ni več mogoče omejiti zgolj na neodobrene transakcije, kot to sicer določa PSD2 (79. uvodna izjava PSR).
Predlog PSR zahteva tudi sodelovanje drugih akterjev v plačilni verigi pri odkrivanju in preprečevanju goljufij, npr.

[10] Uredba EU 2016/679 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov, GDPR.

ponudnikov elektronskih komunikacijskih storitev, kot so operaterji mobilnih omrežij in internetne platforme (81. uvodna izjava predloga PSR). Evropski parlament je sicer v prvi obravnavi predloga PSR sprejel stališče, ki ne predvideva le njihovega sodelovanja, temveč tudi soodgovornost[11]. Izpostaviti pa je treba, da je to stališče prejšnje sestave Evropskega parlamenta.

5.4.1 Različni pristopi v državah članicah

Obstoječe rešitve ponudnikov plačilnih storitev in/ali sodna praksa v državah članicah glede razumevanja, kako manipulacija odobritve vpliva na to, ali se transakcija šteje za odobreno ali ne, so danes različne. Vendar pa države članice v pogovorih v Svetu EU o besedilu predloga PSR izhajajo prav iz svojih nacionalnih rešitev in sodne prakse. Zato je za prihodnjo ureditev ukrepov z zadevnega področja potrebno poznavanje tudi današnjih različnih pristopov v državah članicah.

Iz nemške sodne prakse na primer izhaja, da je plačilna transakcija odobrena pod dvema pogojema: prvič, da plačnik avtenticira plačilno transakcijo, in drugič, da ima tudi namen izvršiti plačilno transakcijo. To pomeni, da mora dati soglasje za izvedbo plačilne transakcije v smislu 64. člena PSD2. V konkretnem primeru je ob predaji oziroma prevzemu elementov za močno avtentikacijo strank plačnik želel posodobiti naprave uporabljene za močno avtentikacijo strank, ne pa dokončati plačilne transakcije, zato jo sodišče šteje za neodobreno. Če se ugotovi, da plačilna transakcija ni bila odobrena, se nato presoja, ali je uporabnik ravnal hudo malomarno, kar pa je ločeno vprašanje od ugotovitve, ali je bila plačilna transakcija odobrena[12]. Iz tega lahko sklepamo, da nemška sodna praksa šteje plačilno transakcijo, ki jo uporabnik odobri zaradi manipulacije (goljufije), za neodobreno.

Po drugi strani iz nizozemske sodne prakse izhaja, da že sama močna avtentikacija plačilne transakcije pomeni njeno odobritev[13]. Vendar so se na Nizozemskem vse večje banke dogovorile in prostovoljno zavezale k shemi za povračila žrtvam goljufij z lažnim predstavljanjem za bančne uslužbence (Dutch Banking Association, 2021). Shema postavlja določene pogoje, ki morajo biti izpolnjeni za povračilo iz sheme, npr. ogoljufani uporabniki morajo prijaviti goljufijo policiji. Moralni hazard uporabnikov preprečuje tudi omejitev, da je vsak uporabnik upravičen do povračila iz te sheme le enkrat v življenju.

[11] Zakonodajna resolucija Evropskega parlamenta z dne 23. aprila 2024 o predlogu uredbe Evropskega parlamenta in Sveta o plačilnih storitvah na notranjem trgu in spremembi Uredbe (EU) št. 1093/2010 (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD)).

[12] LG Halle 4 O 133/22 z dne 23.6.2023; OLG München 19 U 1508/23 e z dne 4.9.2023.

[13] Rechtbank Midden-Nederland UC EXPL 23-8257 z dne 7.8.2024.

6. Mehki ukrepi

6.1 Priporočila ERPB

Na ravni Evropske unije posvečajo pozornost preprečevanju goljufij pri plačilih poleg so-zakonodajalcev tudi druge institucije oz. odbori. Tako je Odbor za plačila malih vrednosti v evrih (ang. Euro Retail Payments Board; ERPB) maja 2023 vzpostavil delovno skupino za naraščanje goljufij, povezanih s plačili malih vrednosti. Delovna skupina je septembra 2024 objavila poročilo o delu ter predvidene ukrepe za preprečevanje in zmanjševanje goljufij (ERPB, 2024).

Poročilo se osredotoča na to, kako znotraj EU celovito reševati problematiko goljufij pri plačilih. Predlogi vključujejo osemnajst ukrepov z različnimi roki, pri čemer je vsak naslovljen na (skupino) specifičnih deležnikov v verigi plačil malih vrednosti na lokalni, nacionalni ali evropski ravni. V poročilu so predstavljeni štirje stebri ukrepov (ang. t. i. game changerji), ki se nanašajo na različna vsebinska področja (ERPB, 2024).

a. **Medsektorsko sodelovanje in odgovornost:** vzpostavitev mreže oz. pobude na ravni EU, ki naj vključuje vse relevantne deležnike v plačilni verigi z namenom olajšanja sodelovanja tako na nacionalni ravni kot tudi na ravni EU. Sekretariat ERPB bo koordiniral nadaljnje ukrepe med relevantnimi organi EU – do junija 2025 se bo določilo, »kdo« in »zakaj«, cilj pa je, da se medsektorsko sodelovanje na ravni EU vzpostavi do konca leta 2025.
b. **Izmenjava podatkov o goljufijah:** vzpostavitev platforme za izmenjavo podatkov na ravni celotne EU, ki bi temeljila na že obstoječih rešitvah/mrežah (npr. platforma EPC za izmenjavo informacij o zlonamerni programski opremi) in izkoriščala pristop t. i. mreže mrež (ang. *network of network approach*). Namen tega je zagotoviti, da bodo obstoječe in bodoče nacionalne platforme za izmenjavo podatkov spodbujene k povezovanju s skupnostjo ponudnikov plačilnih storitev v vseevropski mreži za izmenjavo podatkov, da bodo lahko ti v realnem času dostopali do podatkov, ki so na voljo ponudnikom plačilnih storitev po vsej EU.
c. **Medsektorsko sodelovanje pri izvajanju nadzora na ravni EU**: izmenjava znanja med nadzorniki za zagotavljanje ažurnosti glede trendov goljufi, kar vključuje tudi razmislek o predlogu za vzpostavitev posebne skupine za goljufije ter njihovo odkrivanje in preprečevanje.
d. **Varno oblikovanje produktov:** uporaba izboljšanih varnostnih ukrepov za zaščito potrošnikov, zlasti še pred uvedbo novih produktov, ter redno izvajanje skrbne ocene tveganja goljufij.

Na ravni EU se torej želi oblikovati mreža oz. skupina za preprečevanje goljufij, podpira se izmenjava podatkov glede goljufij ter dodatno analizira, kako bo razvoj tehnologij vplival na goljufije. V Sloveniji smo tokrat pred EU, saj smo že začeli z določenimi aktivnostmi in povezovanjem na nacionalni ravni, o čemer več v naslednjem poglavju.

6.2 Strategija razvoja trga plačil v Sloveniji za obdobje 2024–2028

V okviru Nacionalnega sveta za plačila (NSP), ki deluje od leta 2013 in ga je Banka Slovenije ustanovila kot strateško, posvetovalno platformo deležnikov trga plačil v Sloveniji, je bil sprejet dokument Strategija razvoja trga plačil v Sloveniji za obdobje 2024–2028 (Strategija NSP), ki opredeljuje strateške iniciative NSP (NSP, 2023). Med drugim je cilj Strategije NSP tudi povečanje zaupanja uporabnikov v varnost elektronskih načinov plačevanja. NSP namreč podpira prizadevanja za večjo varnost na področju plačil, potencialno tudi vpeljavo dodatnih varnostnih mehanizmov znotraj rešitev za elektronsko plačevanje, v skladu s potrebami uporabnikov.

Za večjo ozaveščenost uporabnikov na področju varnosti elektronskih načinov plačevanja pa NSP spodbuja aktivno, med deležniki usklajeno in osredotočeno izobraževanje uporabnikov, predvsem o vrstah možnih zlorab ter odgovornosti uporabnikov in načinov za njihovo preprečevanje. Zato je NSP med drugim vzpostavil tudi delovno skupino za ugotavljanje varnostnih vidikov elektronskih plačil, katere naloga je pripraviti nabor ukrepov za posamezne strateške iniciative ter izvesti aktivnosti v letih 2024–2026. Delovna skupina se pri svojem delu osredotoča na sodelovaje med deležniki pri ozaveščanju ter tehničnih rešitvah (NSP, 2024).

7. Sklep

Med temelji Evrosistemove strategije za mala plačila sta varnost in zaščita plačil z zahtevo po najvišji ravni preprečevanja goljufij in varstvu potrošnikov z robustnim postopkom za pritožbe in povračila. Pri preprečevanju goljufij je ključna preventiva (ozaveščanje, spremljanje transakcij v realnem času in drugi s tem povezani ukrepi, kot so moča avtentikacija strank, preverjanje prejemnika plačila ter vzpostavitev pravne podlage za izmenjavo podatkov o goljufivih transakcijah). Vendar pa je, če do goljufije pride, povračilo žrtvam pomemben del zagotavljanja, da ogoljufani uporabniki ohranijo zaupanje v digitalno plačevanje. In pri tem je treba upoštevati tudi pravično razporeditev odgovornosti za goljufije ter s tem pravično razporediti finančno breme goljufij.

PSD2 je z ukrepom močne avtentikacije strank dosegla zavidljive rezultate in krepko znižala število in obseg določenih pojavnih oblik goljufivih plačilnih transakcij. Vendar so goljufi agilni in njihova inovativnost prilagajanja novim oblikam plačevanja in družbenim pojavom ne počiva. Upoštevanje obeh navedenih okoliščin pojasni statistike EBA in ECB, narejene na podlagi poročil ponudnikov plačilnih storitev o goljufijah, da število goljufij pri plačilih na ravni EU ostaja na stabilni ravni. Ne glede na to pa morajo ponudniki plačilnih storitev, regulatorji in uporabniki področje še naprej aktivno spremljati in se hitro odzivati na spremembe trendov (EBA in ECB, 2024).

Kot že navedeno, se modaliteta goljufij hitro spreminja oziroma prilagaja novim razmeram (priložnostim) na trgu, goljufije postajajo vedno bolj sofisticirane. Zato je pri sprejemanju nove zakonodaje na tem področju posebna pozornost namenjena zapisu določb na način, da bodo te uporabne tudi v prihodnosti in v primeru novih pojavnih oblik goljufij. V ilustracijo tega naj navedeva, da je bilo v okviru PSD2 hranjenje PIN-kode skupaj s plačilno kartico v denarnici razumljeno kot primer hude malomarnosti potrošnika (72. uvodna izjava PSD2), vendar ta primer danes kaže pretekle vzorce plačilnih goljufij. V luči agilnosti in čedalje večje sofisticiranosti goljufij pri plačilih je zato nujen skrben premislek, kako pri oblikovanju novega pravnega okvirja, torej predloga PSR, reševati z ukrepi deležnikov trga plačil to konstantno spreminjanje in pripraviti določbe predloga PSR, ki bodo ostale relevantne tudi v nedoločeni prihodnosti, da bodo torej *future-proof*. Hitro spreminjajoče se modalitete goljufij pri plačevanju zahtevajo nadaljnjo pozornost in skupna prizadevanja vseh deležnikov trga za spopadanje z njimi ter s tem posledično za ohranjanje zaupanja uporabnikov plačilnih storitev.

Literatura in viri:

- BIS, 2023. Digital fraud and banking: supervisory and financial stability implications. [Elektronski]
- Dosegljivo na: https://www.bis.org/bcbs/publ/d558.pdf [Dostop 5. 12. 2024].
- Dutch Banking Association, 2021. Criteria for awarding compensation for loss arising from bank help desk scams (»spoofing«). [Elektronski]
- Dosegljivo na: https://www.nvb.nl/media/5661/criteria-for-awarding-compensation-for-loss-arising-from-bank-help-desk-scams-spoofing-june-2nd-2021.pdf [Dostop 5. 12. 2024]
- EBA in ECB, 2024. 2024 Report on payment fraud. [Elektronski]
- Dosegljivo na: https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202408.en.pdf [Dostop 5. 12. 2024]
- EBA, 2022. Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on

payment services in the internal market (PSD2). [Elektronski] Dosegljivo na: https://www.eba.europa.eu/sites/default/files/document_library/Publications/Opinions/2022/Opinion%20od%20PSD2%20review%20%28EBA-Op-2022-06%29/1036016/EBA%27s%20response%20to%20the%20Call%20for%20advice%20on%20the%20review%20of%20PSD2.pdf [Dostop 5. 12. 2024].

- EBA, 2023. Consumer trends report 2022/23. [Elektronski] Dosegljivo na: https://eba.europa.eu/sites/default/files/document_library/Publications/Reports/2023/1054879/Consumer%20Trends%20Report%202022-2023.pdf [Dostop 5. 12. 2024].
- EBA, 2024. EBA Opinion on new types of payment fraud and possible mitigants. [Elektronski] Dosegljivo na: https://eba.europa.eu/sites/default/files/2024-04/363649ff-27b4-4210-95a6-0a87c9e21272/Opinion%20on%20new%20types%20of%20payment%20fraud%20and%20possible%20mitigations.pdf [Dostop 5. 12. 2024].
- ECB, 2023. Card fraud in Europe declined notably in 2021 amid the implementation of regulatory measures [Elektronski] Dosegljivo na: https://www.ecb.europa.eu/press/cardfraud/html/ecb.cardfraudreport202305~5d832d6515.en.html [Dostop 5. 12. 2024].
- Evropska komisija, 2023. Predlog Uredbe Evropskega parlamenta in Sveta o plačilnih storitvah na notranjem trgu in dopolnitvi Uredbe (EU) št. 1093/2010. [Elektronski] Dosegljivo na: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0367 [Dostop 5. 12. 2024].
- Evropska komisija, 2023. Predlog Direktive Evropskega parlamenta in Sveta o plačilnih storitvah in storitvah elektronskega denarja na notranjem trgu, spremembi Direktive 98/26/ES ter razveljavitvi direktiv (EU) 2015/2366 in 2009/110/ES. Dosegljivo na: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0366 [Dostop 5. 12. 2024]
- Evropska komisija, 2020. Sporočilo Komisije Evropskemu Parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij o strategiji EU za mala plačila. [Elektronski] Dosegljivo na: https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:52020DC0592 [Dostop 5. 12. 2024].
- ERPB, 2024. Report of the ERPB Working Group on fraud related to payments. [Elektronski] Dosegljivo na: https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/21st-ERPB-meeting/Report_from_the_ERPB_Working_Group_on_fraud_prevention.pdf [Dostop 5. 12. 2024]
- Evropski parlament, 2023. Zakonodajna resolucija Evropskega parlamenta z dne 23. aprila 2024 o predlogu uredbe Evropskega parlamenta in Sveta o plačilnih storitvah na notranjem trgu in spremembi Uredbe (EU) št. 1093/2010 (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD)). [Elektronski] Dosegljivo na: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0298_SL.html#title1 [Dostop 5. 12. 2024]
- Landesgericht Halle, 2023: 4 O 133/22 z dne 23.6.2023. [Elektronski] Dosegljivo na: https://www.landesrecht.sachsen-anhalt.de/bsst/ document/NJRE001547379 [Dostop 5. 12. 2024]
- Nacionalni svet za plačila, 2024. Potrjen zapisnikI 32. in 33. seje NSP. [Elektronski] Dosegljivo na: https://www.bsi.si/placila-in-infrastruktura/nacionalni-svet-za-placila/gradiva/potrjeni-zapisniki-sej-nacionalnega-sveta-za-placila [Dostop 5. 12. 2024]
- Nacionalni svet za plačila, 2023. Strategija razvoja trga plačil v Sloveniji za obdobje 2024-2028. [Elektronski] Dosegljivo na: https://www.bsi.si/placila-in-infrastruktura/nacionalni-svet-za-placila/gradiva/temeljni-dokumenti-nacionalnega-sveta-za-placila [Dostop 5. 12. 2024]
- Oberlandesgericht München, 2023: 19 U 1508/23 e z dne 4.9.2023. [Elektronski] Dosegljivo na: https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2023-N-28101 [Dostop 5. 12. 2024]
- Rechtbank Midden-Nederland, 2024: UC EXPL 23-8257 z dne 7.8.2024. [Elektronski] Dosegljivo na: https://semantius.nl/uitspraken/ECLI:NL:RBMNE:2024:4459 [Dostop 5. 12. 2024]
- SI-CERT, 2024. Statistika SI-CERT za prvo polovico leta 2024. [Elektronski] Dosegljivo na: https://www.cert.si/statistika-si-cert-za-prvo-polovico-leta-2024/ [Dostop 5. 12. 2024].
- Uradni list Evropske unije, 2015. Direktiva (EU) 2015/2366 Evropskega parlamenta in Sveta z dne 25. novembra 2015 o plačilnih storitvah na notranjem trgu, spremembah direktiv 2002/65/ES, 2009/110/ES ter 2013/36/EU in Uredbe (EU) št. 1093/2010 ter razveljavitvi Direktive 2007/64/ES (UL L št. 337 z dne 23. 12. 2015, str. 35)
- Uradni list Evropske unije, 2024. Uredba (EU) 2024/886 Evropskega parlamenta in Sveta z dne 13. marca 2024 o spremembi uredb (EU) št. 260/2012 in (EU) 2021/1230 ter direktiv 98/26/ES in (EU) 2015/2366 glede takojšnjih kreditnih prenosov v eurih (UL L št. 2024/886 z dne 19. 3. 2024)
- Uradni list Evropske unije, 2021. Uredba (EU) 2021/1230 Evropskega parlamenta in Sveta z dne 14. julija 2021 o čezmejnih plačilih v Uniji (kodificirano besedilo) (UL L št. 274 z dne 30. 7. 2021, str. 20)
- Uradni list Evropske unije, 2018. Delegirana uredba Komisije (EU) 2018/389 z dne 27. novembra 2017 o dopolnitvi Direktive (EU) 2015/2366 Evropskega parlamenta in Sveta glede regulativnih tehničnih standardov za močno avtentikacijo strank ter skupnih in varnih odprtih standardov komunikacije (UL L št. 69 z dne 13. 3. 2018, str. 23)
- Uradni list Evropske unije, 2016. Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L št. 119/1 z dne 4. 5. 2016)
- Uradni list RS, 1997. Obligacijski zakonik. Uradni list RS, št. 97/07 – uradno prečiščeno besedilo, 64/16 – odl. US in 20/18 – OROZ631
- Uradni list RS, 2018. Zakon o plačilnih storitvah, storitvah izdajanja elektronskega denarja in plačilnih sistemih, Uradni list RS, št. 7/18, 9/18 – popr. in 102/20
- Vrhovno sodišče, 2020. VSRS Sodba III Ips 62/2019. [Elektronski] Dosegljivo na: https://www.sodnapraksa.si/?q=*:*&database%5bSOVS%5d=SOVS&database%5bIESP%5d=IESP&database%5bVDSS%5d=VDSS&database%5bUPRS%5d=UPRS&_submit=išči&id=2015081111441129 [Dostop 5. 12. 2024].
- ZBS, 2024. Elektronsko identiteto je treba skrbno varovati, sporočilo za javnost. [Elektronski] Dosegljivo na: https://www.zbs-giz.si/elektronsko-identiteto-je-treba-skrbno-varovati-sporocilo-za-javnost/ [Dostop 5. 12. 2024].