



Mnenja IRPS od 1.1.2025 dalje

Mnenje v sporu zaradi vračila kredita – 7.1.2025

Pobudnica navaja, da je bila dne 16.7.2024 ųrtev spletne prevare oziroma zlorabe. Neznanec jo je poklical po telefonu in jo nagovoril, da izkoristi moųnost dviga 5.000,00 EUR, kolikor naj bi znašal dobiček od njenega nakupa kriptovalute v letu 2020. Nato jo je vodil skozi postopek nakazila sredstev, pri čemer je od nje zahteval podatke o plačilni kartici, vključno z njeno številko in časovno veljavnostjo. Napeljal jo je tudi, da je namestila aplikacijo Simplex. Pobudnica podrobno opisuje nadaljnje dogajanje, ki se je končalo s tem, da je ugotovila, da se je znesek limita na njenem računu zvišal od 700,00 EUR na 5.200,00 EUR, prejela pa je tudi obvestilo o odobritvi kredita in povišanju limita, čeprav nikoli ni bila o tem obveščena v pisni obliki ali na kakšen drug način.

Dne 18.7.2024 se je pobudnica oglasila v poslovalnici banke v Murski Soboti, kjer so nemudoma blokirali njeno plačilno kartico. Zlorabo plačilne kartice je naznanila tudi policijski postaji Murska Sobota.

Pobudnica navaja, da sta bili zvišanje limita in sklenitev osebnega kredita izvedeni iz tujega IP naslova. Skupaj je bilo izvedenih sedem transakcij v skupnem znesku 19.000,00 EUR, šlo pa je za neodobrene plačilne transakcije. V svojem ravnanju ne vidi ničesar hudo malomarnega. V zvezi s tem se sklicuje tudi na sodno prakso.

Pobudnica dodaja, da banka ni ravnala v skladu z določbo 3. odst. 47. člena ZBan-3 in tudi ne v skladu z določbo 10. člena ZPotK-2. Meni, da sta tako kreditna pogodba kot pogodba o izrednem limitu izpodbojni, saj pobudnica ni bila obveščena in niti ni mogla vedeti, da sklepa navedeni pogodbi. Banka bi kot nasprotna stranka pogodbenega razmerja morala biti seznanjena z dejstvom, da je tretja oseba pobudnico zavedla v zmoto, posledično v prevaro. S sklicevanje na določbo 96. člena OZ zahteva, da se ji vrne vse, kar je bilo pridobljeno na podlagi navedenih pogodb.

Banka zavrača zahtevek pobudnice. Poudarja, da je do zlorabe lahko prišlo, ker je pobudnica neznanim osebam omogočila oddaljen dostop do svoje naprave. S tem jim je dejansko omogočila, da pridobijo dostop do njenih osebnih/kartičnih podatkov in banke Klik, kar jim je omogočilo, da so izvedli transakcije, kot so najem kredita in zvišanje izrednega limita, v nadaljevanju pa spletne nakupe. Z oddaljenim dostopom je bilo „zlobcem“ tudi omogočeno pregledovanje e-pošte. Banka ni odgovorna za zlorabo, saj so tretje osebe pridobile dostop do podatkov pobudnice po njeni privolitvi, saj si je aplikacijo za oddaljen dostop pobudnica naložila sama. Ko je dovolila oddaljen dostop do svoje naprave, so te osebe lahko delovale, kot da izvaja transakcije sama pobudnica, saj so imele dostop do njenih bančnih storitev.

Za banko je ključno, da uporabnik storitve (pobudnica) vedno pazi na to, kdo ima dostop do njenih naprav in osebnih podatkov. Omogočen oddaljen dostop do njene naprave neznanim osebam je podoben temu, kot če bi kriminalcem predali ključke od svojega doma. V takih



primerih banka žal ne more preprečiti zlorabe. Banka vseskozi seznanja stranke in jih obvešča, da je bilo v zadnjem času zaznано povečano število finančnih zlorab. Zato stranke poziva k varovanju osebnih podatkov, previdnosti in da naj ne nalagajo neznanih aplikacij na svojo napravo. Pobudnici je takšna opozorila poslali dne 28.3.2024 in dne 10.5.2024, nekaj pa jih je bilo poslano tudi pred 28.3.2024.

Ko so neznane osebe s pomočjo aplikacije za oddaljen dostop vstopile v pobudničin Klik, so v nadaljevanju:

1. najeli kredit v višini 15.900,00 EUR. Ob najemu so nastali dodatni stroški:

- premija za življenjsko zavarovanje v višini 792,75 EUR,
- strošek ocene tveganja v višini 694,16 EUR,
- interkalarnе obresti v višini 45,05 EUR in
- stroški odobritve v višini 125,00 EUR.

2. najeli izredni limit v višini 5.200,00 EUR. Ob tem so nastali stroški:

o nadomestilo za obravnavo limita v višini 161,20 EUR in

o zavarovalna premija za limit v višini 46,80 EUR.

3. izvedli 7 kartičnih plačil v različnih zneskih v skupni višini 19.000,00 EUR.

V zvezi s sklenitvijo kreditne pogodbe in izrednega limita banka pojasnjuje, da je zahtevek za sklenitev le-teh bil podan preko spletnega Klika pobudnice dne 16.7.2024. V takšnem primeru se po njenem mnenju šteje, da je naročilo za kredit/limit podal uporabnik spletne banke in da je uporabnik sklenil posel/podpisal pogodbo. Vstop v spletni banki je namreč mogoč le z uporabniškim imenom, ki ga pozna izključno uporabnik in enkratnim geslom, ki ga generira uporabnik na svojem telefonu. Navedba pobudnice, da ji dokumentacija ob sklenitvi kredita in limita ni bila posredovana v nobeni obliki, ne drži. Iz sistemskih izpisov je razvidno, da so bili dokumenti ob sklenitvi kredita in limita posredovani na elektronski naslov pobudnice, kakor tudi na njeno mobilno številko.

Na očitek, da ni ugotavljala kreditne sposobnosti pobudnice, banka odgovarja, da ugotavlja kreditno sposobnost skladno z veljavno zakonodajo in makrobonitentimi omejitvami financiranja potrošnikov. Glede na podatke pobudnice je bila slednja ob odobritvi obeh poslov kreditno sposobna.

V nadaljevanju banka podrobno navaja vstopе v Klik, ki so bili opravljeni med 18:42:28 in 21:58:02. Iz spiska je razvidno, da je bilo devet vstopov v mobilni Klik opravljenih z naprave, ki naj bi bila po trditvah pobudnice njena, tri vstopе v spletni Klik pa iz neznane naprave.

Vse transakcije, ki jim pobudnica oporeka, naj bi bile potrjene v elektronski denarnici pobudnice med 19:40:53 in 19:54:49, v skupni vrednosti 19.000,00 EUR.

Pobudnici je banka želela pomagati in je prodajnima mestoma v sodelovanju s procesnim centrom Bankart d.o.o. poslala finančne reklamacije zaradi zlorabe, kar pa ni bilo uspešno, ker so bile transakcije pred avtorizacijo potrjene v elektronski denarnici pobudnice. Pojasnjuje, da za take transakcije pod nobenim pogojem prodajnemu mestu ni mogoče poslati finančne reklamacije zaradi zlorabe.

Za prvo transakcijo v višini 2.500,00 EUR je banka pobudnici na njeno telefonsko številko poslala SMS sporočilo z vsebino:

»Pozdravljeni, na vaši kartici ****8698 smo zaznali transakcijo SPLET NAKUP, 16.07.2024 19:39:38, Revolut**8392*, 2.500,00 EUR in kartici omejili poslovanje. Če ste transakcijo opravili sami, odgovorite POTRDI in kodo 92 (primer: POTRDI 92).«.



Potrditveni SMS s pravilno vsebino je pobudnica poslala banki in s tem potrdila, da plačilo res izvaja sama. Prav tako ji je bilo ob 19:43:19 uri poslano sporočilo za transakcijo 3.000,00 EUR in je prejela potrditveni SMS od pobudnice.

Škoda, ki jo je utrpela pobudnica, je po stališču banke posledica njenega posredovanja osebnih in varnostnih podatkov tretji osebi. Navedeno predstavlja kršitev določil 132. člena ZPlaSSIED, ki določa, da mora uporabnik uporabljati plačilni instrument v skladu s pogoji, ki urejajo izdajo in uporabo plačilnega instrumenta ter takoj po prejemu plačilnega instrumenta zagotoviti vse razumne ukrepe, da zavaruje osebne varnostne elemente plačilnega instrumenta. V skladu z določili 3. odstavka 137. člena v povezavi s prej navedenim 132. členom ZPlaSSIED v takšnem primeru uporabnik odgovarja za celotni znesek neodobrene plačilne transakcije.

Ker med pobudnico in banko ni bil dosežen sporazum o rešitvi spora, izdaja posrednik v sporu na podlagi določbe drugega odstavka 14. člena Pravil postopka za izvensodno reševanje potrošniških sporov pri Združenju bank Slovenije naslednje

nezavezujoče mnenje o spornem razmerju:

Pobuda ni utemeljena

Iz skope predstavitve banke, kako sta bili sklepani pogodbi o zvišanju limita in o osebnem kreditu, je mogoče sklepati, da je šlo za postopek, ki so ga generirali računalniški algoritmi. Nobenih trditev ni o izpolnjevanju dolžnosti banke po določbah Zakona o potrošniških kreditih (ZPotK-2). V 3. odstavku 7. člena je npr. določeno, da dajalec kredita potrošniku pisno na papirju ali drugem trajnem nosilcu podatkov pravočasno pred sklenitvijo kreditne pogodbe brezplačno zagotovi predhodne informacije o kreditni pogodbi, na podlagi katerih potrošnik lahko primerja različne ponudbe in presodi ustreznost kreditne pogodbe glede na svoje potrebe in finančni položaj. V 10. členu je določena dolžnost banke, da oceni kreditno sposobnost potrošnika, kar napravi na podlagi potrebnih, zadostnih in sorazmernih informacij o prihodkih in izdatkih oziroma premoženjskem stanju potrošnika, ki jih pridobi od potrošnika in iz zbirk osebnih podatkov iz tretjega odstavka istega člena. O poizvedbi v zbirki osebnih podatkov je treba potrošnika predhodno obvestiti (3. odstavek 10. člena). Če bi banka ravnala v skladu z navedenimi določbami ZPotK-2, bi neizogibno morala komunicirati s pobudnico že pred samo sklenitvijo pogodb, pogodbi pa po vsej verjetnosti ne bi mogli skleniti prevaranti v imenu pobudnice (ker ne bi poznali vseh potrebnih podatkov in bi sklepanje zahtevalo več časa, kot ga imajo na voljo, da se prevara pravočasno ne odkrije in prepreči).

Ni pa mogoče pritrditi pobudnici, ki se sklicuje na določbo 96. člena Obligacijskega zakonika, ko zahteva, da se ji „vrne vse, kar je bilo pridobljeno na podlagi navedenih pogodb“. Na podlagi kreditne pogodbe je ona prejela denarna sredstva, ne banka. Vrnitvena dolžnost v primeru neveljavne pogodbe bi zato zadelo njo in ne banko.

Pobudnica se sklicuje na spletno prevaro, a je šlo dejansko za telefonsko prevaro, s pomočjo spleta je bila prevara (tvezenje neznancev, da bo prejela 5000,00 EUR) le izpeljana.

Banka pravilno opozarja na določbo 132. člena ZPlaSSIED, ki določa, da mora uporabnik uporabljati plačilni instrument v skladu s pogoji, ki urejajo izdajo in uporabo plačilnega instrumenta ter takoj po prejemu plačilnega instrumenta zagotoviti vse razumne ukrepe, da



zavaruje osebne varnostne elemente plačilnega instrumenta. Manj prepričljivo (nepopolno) je njeno sklicevanje na določbo 3. odstavka 137. člena, po kateri naj bi v povezavi s prej navedenim 132. členom ZPlaSSIED, v takšnem primeru uporabnik odgovarjal za celotni znesek neodobrene plačilne transakcije. Po navedeni določbi uporabnik odgovarja, če je izvršitev neodobrene plačilne transakcije posledica njegove prevare ali goljufije, ali če zaradi hude malomarnosti ni izpolnil ene ali več obveznosti v zvezi s plačilnim instrumentom v skladu s 132. členom. Za odgovornost pobudnica za celotno izgubo zaradi neodobrenih transakcij, je zato treba v tem primeru oceniti, ali je ravnala hudo malomarno, ko je neznancu zaupala podatke, ki bi jih morala varovati po določbi 132. člena ZPlaSSIED (osebne varnostne elemente plačilnega instrumenta). Hudo malomarno ravna tisti, ki ravna skrajno nepazljivo, tako kot ne bi ravnal noben razumen človek v enaki dejanski situaciji.

Pobudnica je zaupala osebi, ki je ni poznala in jo je nagovorila po telefonu s slabim znanjem slovenščine, torej popolnemu neznancu, podatke svoje bančne kartice in na telefon namestila njej neznano aplikacijo, ki je omogočala oddaljen dostop do njene elektronske naprave. Zakaj je tako ravnala kljub pogostim pozivom banke k varovanju osebnih podatkov, previdnosti in proti nalaganju neznanih aplikacij na svoje naprave? Razlog, ki ga ponuja, naj bi bil v tem, ker je neznancu verjela, da ji bo zagotovil izplačilo dobička, ki naj bi ga ustvarila z nakupom kriptovalut v letu 2020. Splošna življenjska izkušnja pove, da uporabljamo bančno kartico tedaj, ko nekaj plačujemo, torej ko razpolagamo z denarnimi sredstvi, ne pa tedaj, ko prejemamo plačilo. Enako velja za nekakšno aplikacijo, ki naj bi bila potrebna za prejem denarnega zneska.

Iz zapisnika, sestavljenega na Policijski postaji Murska Sobota, je razvidno, da je pobudnica zaznala, da je neznanec nekaj počel v spletni banki brez njenega sodelovanja in je posumila, „da bi lahko bilo kaj narobe“ v postopku, ki je trajal kakšno uro. Prejela je sporočilo banke, s katerim je bila zaprosena, da podpiše kreditno pogodbo in zvišanje limita. Kljub temu se očitno ni obrnila na banko za pojasnilo, saj tudi naslednjega dne ni dvignila slušalke, ko je prejela klic iz banke. Celotno ravnanje je v taki meri nerazumno, da dosega stopnjo hude malomarnosti, kar pomeni, da po določbi 132. člena ZPlaSSIED odgovarja za celotni znesek neodobrenih plačilnih transakcij sama in ne banka.

Mnenje v sporu zaradi neveljavnosti kreditne pogodbe – 7.1.2025

Pobudnica zatrjuje, da jo banka neupravičeno bremeni za vrnitev kredita. Kreditno pogodbo naj bi stornirala, sam kredit pa ji naj bi bil odtujen. Zanja je vprašljiva tudi hitra odobritev kredita osebi, ki ji je denar odtujila, saj je z naknadnim preverjanjem ugotovila, da se kredit ne bi smel niti odobrit zaradi kreditne nesposobnosti. Na naroku je povedala, potem ko ji je bila predložena kreditna pogodba, da podpis ni njen.

Banka je odgovorila, da je pobudnica dne 21.05.2024 pri kreditnemu posredniku LEVEL INVEST d.o.o., Cesta zmage 73, Maribor sklenila kreditno pogodbo za potrošniški kredit za nakup vozila. Kredit je bil istega dne v celoti črpan in na podlagi računa nakazan kreditnemu posredniku, pri katerem je pritožnica tudi kupila vozilo. Dne 04.06.2024 je pritožnica odstopila od Kreditne pogodbe, pri čemer je navajala, da naj bi šlo pri postopku nakupa vozila za prevaro, saj vozila ni prejela. Banka je uvedla interno preiskavo kreditnega procesa, o uvedbi katere je bila pritožnica obveščena, in pričela s postopkom ureditve odstopa od Kreditne pogodbe.



Po izvedeni interni preiskavi banka ni ugotovila nobenih nepravilnosti na njeni strani pri sklepanju kreditne pogodbe. Pritožnica je bila zato dne 24.07.2024 z dopisom pozvana, da vrne celoten znesek črpanega kredita z natečenimi obrestmi. V skladu s tretjim odstavkom 18. člena ZPotK-2 je namreč potrošnik, ki po črpanju kredita odstopi od kreditne pogodbe, dolžan v roku 30 dni od datuma odstopa vrniti celoten znesek glavnice z natečenimi pogodbenimi obrestmi, ki tečejo od datuma črpanja kredita dalje. Pritožnica do datuma priprave tega odgovora dolgovanega zneska še ni vrnila.

Na naroku je pooblaščenec banke navedel, da trenutno za pobudnico ni nobenih negativnih posledic, ima pa banka odprto terjatev do nje za glavnico.

Ker med pobudnico in banko ni bil dosežen sporazum o rešitvi spora, izdaja posrednik v sporu na podlagi določbe drugega odstavka 14. člena Pravil postopka za izvensodno reševanje potrošniških sporov pri Združenju bank Slovenije naslednje

nezavezujoče mnenje o spornem razmerju:

Utemeljenost pobude je odvisna od odgovora na vprašanje, ali je bila kreditna pogodba veljavno sklenjena.

Če pobudnica ni izrazila volje za sklenitev kreditne pogodbe (je ni podpisala in je posrednik ponaredil njen podpis, da bi pridobil znesek kredita), pogodba (njen zapis) zanjo ni zavezujoča in lahko banka zahteva vrnitev kredita le od posrednika.

Če bi se izkazalo nasprotno, je pobudnica banki dolžna vrniti znesek kredita, ki je bil nakazan posredniku, čeprav ta pobudnici ni izročil vozila, ki je bil plačan s pomočjo bančnega kredita.

V tem postopku ni bilo mogoče odgovoriti na zgoraj zastavljeno vprašanje brez pritegnitve posrednika, ki pa se po navedbi banke sploh ne odziva na njene klice.

Mnenje v sporu zaradi spletne zlorabe – 7.1.2025

Pobudnica zahteva povrnitev zneska transakcije z dne 23. 9. 2024 v višini 630,00 EUR. Transakcija je bila izvedena z njeno Mastercard kartico pri nakupu preko prodajnega mesta »BIFINITY«. Znesek v višini 30, 00 EUR predstavlja nadomestilo za transakcije "Quasi Cash". Pobudnica zatrjuje, da navedene transakcije ni opravila, niti ni nikogar pooblastila, da opravi nakup namesto nje. Kartice ni izgubila, niti ji ni bila ukradena, ves čas jo je imela pri sebi.

Banka, ki zavrača zahtevo, da ponudnici povrne znesek 630,00 EUR, pojasnjuje, da je šlo pri navedeni transakciji za zavarovano spletno transakcijo. Za transakcijo je avtentikacijo izvedla pritožnica sama v Rekono OnePass aplikaciji. Pritožnica je bila o transakciji obveščena s SMS sporočilom na svojo telefonsko številko. Kot je razvidno iz slike zaslona iz avtorizacijskega sistema, je pritožnica opravila najprej transakcijo v višini 650,00 EUR, ki pa je bila zavrnjena. Pet minut kasneje je bila ponovno opravljena transakcija v višini 600,00 EUR, ki je bila potrjena v Rekono OnePass aplikaciji.

Iz dokumentacije in podatkov, vezanih na sporno transakcijo, po mnenju banke izhaja, da je mogoče v obravnavanem primeru pobudnici očitati, da ni postopala v skladu z določili Splošnih pogojev poslovanja z Addiko kartico Mastercard glede varovanja kartice pred zlorabo ter da je ravnala s hudo malomarnostjo, v posledici katere je prišlo do zlorabe njene Mastercard



kartice ter oškodovanja v skupnem znesku 630,00 EUR.

Banka še pojasnjuje, da znesek v višini 30,00 EUR predstavlja nadomestilo za transakcije "Quasi Cash". Nadomestilo za transakcije "Quasi Cash" se zaračuna vedno, kadar prodajno mesto v obračun pošlje transakcijo s kodo, ki opredeljuje "Quasi Cash" transakcijo. Splošni pogoji v poglavju »Splošno in opredelitev pojmov« opredelijo pojem "Quasi Cash" in da se nadomestilo za transakcije "Quasi Cash" zaračuna v skladu z vsakokrat veljavnim Cenikom. Cenik storitev za področje poslovanja z občani, veljaven od 02.09.2024, določa, da nadomestilo znaša 5,00 % od zneska transakcije.

Ker med pobudnico in banko ni bil dosežen sporazum o rešitvi spora, izdaja posrednik v sporu na podlagi določbe drugega odstavka 14. člena Pravil postopka za izvensodno reševanje potrošniških sporov pri Združenju bank Slovenije naslednje

nezavezujoče mnenje o spornem razmerju:

Pobuda ni utemeljena.

Pobudnica ni odgovorila na trditve banke, postavljene v odgovoru na njeno pobudo. Poleg tega se trditve banke skladajo s splošno sprejetim prepričanjem, na katerem temelji celotno kartično poslovanje, namreč, da sama bančna kartica, tudi če bi do nje na kakršenkoli način prišla druga oseba, še ne omogoča plačevanja.

Po neprerekanih trditvah banke je avtentikacijo transakcijo izvedla pobudnica sama v Rekono OnePass aplikaciji. O transakciji je bila obveščena s SMS sporočilom na svojo telefonsko številko. Ob takem dejanskem stanju njeni zahtevi za povrnitev zneska 630,00 EUR ni mogoče pritrditi.

Mnenje v sporu zaradi neodobrenih transakcij – 6.2.2025

Pobudnica je v pobudi navedla samo to, da je prišlo do spletne transakcije v skupnem znesku 30.000,00 EUR. Iz pobudi priložene kazenske ovadbe, ki jo je vložila na Policijski postaji Kamnik, pa je naznanila, da jo je dne 22. 6. 2024 po telefonu poklical neznanec in ji rekel, da ima v krypto valutah 2.300,00 EUR. Čeprav nikoli ni trgovala s krypto valutami, jo je prepričal, da se je denar zaslužil z robotskim trgovanjem. Poslušala je njegova navodila in si na telefon namestila aplikacijo AnyDesk. Storilec je nato zahteval, naj gre v e-banko, kjer se je prijavila in vtiskala svoje geslo. Potem ji je narekoval kje in kaj naj tipka. V tem času po navodilu storilca ni smela gledati sms sporočil, ki so prihajala, češ da ima slab signal. Komunikacija je trajala približno dve uri, ko je bil signal prekinjen. Po ponovnem klicu neznanca ji je ta povedal, da je transakcija ustavljena, ker banka ne dela več. Povedal ji je še, da jo bodo iz banke klicali in naj jim reče, da je vse sama tipkala. Ko je nato pri banki preverjala, koliko ima denarja, so ji povedali, da je njen račun blokiran in da ima kredit v višini 33.000,00 EUR.

Banka v odgovoru na pobudo k navedbam pobudnice dodaja, da so neznane osebe s pomočjo aplikacije za oddaljen dostop vstopile v pobudnično e-banko in najele kredit v višini 26.100,00 EUR, pri čemer so nastali še stroški, vzeli izredni limit v višini 6.700,00 EUR, pri čemer so tudi nastali stroški, izvedli prenos 5.200,00 EUR z varčevalnega računa na osebni račun, nato pa izvedli 12 kartičnih plačil po 2.500,00 EUR na prodajnem mestu Bifinity Deposit. Pri tem banka navaja, da je pobudnici poslala več opozoril o sumljivih transakcijah, pobudnica pa se je odzvala s potrditvenima SMS-oma.



Banka navaja, da je želela pobudnici pomagati in prodajnemu mestu v sodelovanju s procesnim centrom Bankart d.o.o. poslati finančne reklamacije zaradi zlorabe. Te pa žal niso bile možne, saj so bile transakcije potrjene v elektronski denarnici.

Glede na to je banka mnenja, da ne gre za neodobrene transakcije oziroma da pobudnica ni ravnala s skrbnostjo, ki se pričakuje od povprečnega človeka in po oceni banke ni upoštevala niti tistega, kar bi v dani situaciji upošteval vsak, tudi manj skrben človek. Banka zato meni, da je pobudnica ravnala s hudo malomarnostjo, zaradi česar je sama odgovorna za celotno izgubo zneskov skladno z določbo tretjega odstavka 137. člena Zakona o plačilnih storitvah, storitvah izdajanja elektronskega denarja in plačilnih sistemih (ZPlaSSIED, Uradni list RS, št. 7/18, 9/18 – popr. in 102/20).

Banka dodaja še, da vseskozi seznanja stranke in jih obvešča, da je v zadnjem času zaznala povečano število finančnih zlorab ter jih poziva k varovanju osebnih podatkov, previdnosti in da naj ne nalagajo neznanih aplikacij na svojo napravo. Tudi pobudnici je pred obravnavanimi transakcijami poslala šest takih varnostnih opozoril, zadnje 10. 5. 2024.

Na naroku 25. 9. 2024 sta se stranki dogovorili, da bosta poskusili zadevo končati s sporazumom. Vendar pa po večkratnem pozivu posrednika v sporu odgovora pobudnice ni bilo, zaradi česar je posrednik ugotovil, da do sporazuma ni prišlo. Zato je na podlagi določbe drugega odstavka 14. člena Pravil postopka za izvensodno reševanje potrošniških sporov pri ZBS izdal to nezavezujoče mnenje.

Pobuda ni utemeljena.

Ni dvoma, da je pobudnica omogočila neznani osebi, da je z aplikacijo AnyDesk prišla do oddaljenega dostopa do njenega telefona in s tem tudi do dostopa do njene e.banke. Iz njenega opisa dogodkov sledi, da je pobudnica nato po nareku neznanca sama izvedla in avtenticirala vse obravnavane transakcije. V tem primeru gre za odobrene transakcije, za katere banka glede na določbo prvega odstavka 136. člena ZPlaSSIED (skladno s katero plačnikov ponudnik plačilnih storitev (banka) odgovarja za izvršitev plačilne transakcije brez plačnikovega soglasja (neodobrena plačilna transakcija)) ne odgovarja.

Če pa je transakcije preko oddaljenega dostopa do pobudničine spletne banke izvajal neznan storilec, so transakcije neodobrene, saj jih ni odobrila pobudnica. V tem primeru banka načeloma odgovarja za transakcije, svoje (objektivne, ne glede na krivdo) odgovornosti pa se lahko reši, kadar je izvršitev transakcije posledica uporabnikove prevare ali goljufije ali če je uporabnik ravnal naklepno ali zaradi hude malomarnosti (tretji odstavek 137. člena ZPlaSSIED).

Za odločitev o tem, kdo naj nosi škodo, nastalo zaradi transakcij, opravljenih v nasprotju s pobudnikovo voljo, je zato treba odgovoriti na vprašanje, ali je pobudnica kršila pogoje, ki urejajo uporabo plačilnega instrumenta, in pri tem ravnala s hudo malomarnostjo.

S tem, ko je omogočila, da je nekdo tretji z uporabo aplikacije AnyDesk prišel do njene spletne banke, je pobudnica kršila obveznost, ki ji jo v zvezi s plačilnimi instrumenti in osebnimi varnostnimi elementi nalaga določba 132. člena ZPlaSSIED. Ta določa, da uporabnik uporablja plačilni instrument v skladu s pogoji, ki urejajo izdajo in uporabo plačilnega instrumenta ... ter takoj po prejemu plačilnega instrumenta zlasti zagotovi vse razumne ukrepe, da zavaruje osebne varnostne elemente plačilnega instrumenta.

Vprašanje je, ali je pobudnica pri tem ravnala hudo malomarno. Hudo malomarnost predstavlja



ravnanje, pri katerem oseba ravna z manjšo skrbnostjo od skrbnosti, ki se v posameznem primeru pričakuje od vsakega razumnega človeka. Kaj se pričakuje od vsakega razumnega človeka, pa se presoja upoštevajoč okoliščine posameznega primera. Po mnenju posrednika v sporu ravnanje, ko nekdo omogoči neznani osebi oddaljen dostop do njegove spletne banke, odstopa od ravnanja vsakega razumnega uporabnika bančnih storitev in zato ravna s hudo malomarnostjo. V času, ko je opozarjanje na spletne prevare v javnih medijih in preko pogostih opozoril bank izjemno obsežno, je razumno pričakovati, da so uporabniki bančnih storitev s tem dobro seznanjeni, zato je že od manj skrbnega uporabnika mogoče pričakovati, da neznancu ne bo omogočil takega oddaljenega dostopa. Poleg tega ni mogoče prezreti, da je banka pobudnico med potekom transakcij opozarjala na njihovo nenavadnost in jo pozivala, da jih posebej potrdi s potrditvenim SMS-om, kar je pobudnica kar dvakrat tudi storila. Banka torej za obravnavane finančne transakcije ne more biti odgovorna.

Mnenje v sporu zaradi neodobrenih transakcij – 17.2.2025

Pobudnica je v pobudi, poslani z elektronsko pošto dne 13. 11. 2024, navedla samo to, da prosi za podatke, kaj vse se je dogajalo na rekoni od 7. 11. do 9. 11., ker ona transakcij ni potrjevala, ni dobila nobenega sporočila na koliko obrokov, ni nič kupovala, kateri pin je bil uporabljen (ona ga ni spreminjala). Trdila je, da gre za vdor v njene račune in odtegnitev sredstev, za krajo. Na poziv IRPS je pojasnila, za katero banko se gre.

Pobudnica je nato svojo pobudo dopolnila dne 6. 12. 2024. Tam je navedla, da je oddelek za kartično poslovanje banke zavrnil njeno reklamacijo zaradi zlorabe kreditne kartice, češ da je bila transakcija potrjena s strani Rekone z njenim uporabniškim geslom, ki ga je nastavila ob registraciji, kar pa ne drži. Trdi, da je bilo njeno geslo spremenjeno dne 7. 11. ob 10.50, nakar je nekdo zlorabil njen mastercard v višini 1.000,00 EUR. Pobudnica trdi, da gesla ni spremenila in ni opravila transakcij za prodajno mesto Binance.com ter da z digitalnimi valutami ni nikoli trgovala. Odtegnjeno je bilo celo več sredstev, kot je dovoljeno, saj je bilo poleg dveh transakcij v zneskih 950,00 EUR in 50,00 EUR, odtegnjenih še 50,00 EUR, tako da skupna škoda znaša 1.050,00 EUR.

Po navedbah pobudnice je prišlo brez njene vednosti in privolitve še do odtegnitve 370,00 EUR z njene debitne kartice. Opravljen je bil spletni nakup na Bifinity in tega ona ni opravila. Obe kartici sta bili takoj blokirani.

Pobudnica navaja še, da so bila poleg tega opravljena tudi sporna plačila na TRR v zneskih 10,00 EUR, 5,00 EUR in 750,00 EUR. Skupna škoda tako po trditvah pobudnice znaša 2.150,00 EUR. Oškodovanje je prijavila policiji.

Banka v odgovoru na pobudo pojasnjuje, da je šlo pri transakcijah preko spleta za zavarovane spletne transakcije, ki so bile vse potrjene z Rekono SMS OTP močno avtentikacijo. O njih je bila pobudnica obveščena še s SMS sporočilom na njeno telefonsko številko, a je vse transakcije uspešno potrdila preko avtorizacijskega sistema. Pri dveh transakcijah z obročno kartico je šlo za „Quasi Cash“ transakciji, zaradi česar je morala pobudnica plačati tudi stroške v skupni višini 50,00 EUR. O zatrjevani spremembi dostopnega gesla za Rekono je banka navedla, da je ugotovila, da je bilo geslo res zamenjano. Za njegovo zamenjavo pa je bilo treba poznati številko kartice, PIN kodo in dostop do ponudnične elektronske pošte. O zamenjavi gesla je bila po trditvah banke pobudnica obveščena s SMS sporočilom in pozivom, naj banki takoj sporoči, če zamenjave ni opravila sama - tega pobudnica ni storila. Pri tem pa banka pripominja, da je pobudnica v razgovoru z bančno uslužbenko navedla, da je na



mobilno napravo namestila programsko opremo za oddaljen dostop AnyDesk. Glede na to je banka mnenja, da pobudnica ni ravnala s skrbnostjo, ki se pričakuje od povprečno skrbnega človeka, njeno ravnanje pa je bilo v nasprotju z določbami 132. člena Zakona o plačilnih storitvah, storitvah izdajanja elektronskega denarja in plačilnih sistemih (ZPlaSSIED, Uradni list RS, št. 7/18, 9/18 – popr. in 102/20) in s Splošnimi pogoji za vodenje transakcijskega računa in opravljanje plačilnih storitev, s katerimi je predpisano skrbno ravnanje uporabnika kartice. Banka zato meni, da je pobudnica ravnala s hudo malomarnostjo, zaradi česar je sama odgovorna za celotno izgubo zneskov skladno z določbo tretjega odstavka 137. člena ZPlaSSIED. V bistvenem enako meni banka tudi o plačilnih transakcijah v zvezi s takojšnjimi plačili v zneskih 750,00 EUR in 5,00 EUR. Za oba zneska je banka posredovala zahtevek za njuno vračilo. Za znesek 5,00 EUR je prejela odgovor Delavske hranilnice d.d., da prejemnik sredstev zavrača vračilo, za znesek 750,00 EUR pa odgovor Unicredit banke d.d., da se njihova stranka ne odziva.

Banka na koncu predlaga, naj posrednik za izvensodno reševanje potrošniških sporov izda negativno mnenje.

Na naroku 20. 1. 2025 je pobudnica želela ta spor povezati z odplačilom kredita, ki ga ima pri banki in ga zaradi obravnavanega oškodovanja ne more odplačevati. O tem sta se stranki dogovorili, da bosta poskusili vprašanje plačevanja kredita rešiti izven tega postopka. Glede oškodovanj pobudnice do sporazuma med njo in banko ni prišlo. Zato je posrednik v sporu na podlagi določbe drugega odstavka 14. člena Pravil postopka za izvensodno reševanje potrošniških sporov pri ZBS (v nadaljevanju: Pravila) izdal to nezavezujoče mnenje.

Pobuda ni utemeljena.

Postopek posredovanja v potrošniškem sporu je kombiniran posredovalno-predlagalni postopek (prvi odstavek 12. člena Pravil), ki ni primeren za ugotavljanje in dokazovanje zapletenih dejanskih vprašanj: v tem primeru vprašanja, kako je v resnici prišlo do odtujitve pobudničinega denarja. Pobudnica trdi, da ni nikomur dala varovalnih podatkov, potrebnih za uporabo njenih kartic in njene mobilne banke. Banka pa prepričljivo opisuje, da so bile transakcije izvedene z močno avtentikacijo, za katero zgleda, kot da jo je opravila pobudnica. Pri tem opozarja, da je pobudnica njeni uslužbenki v telefonskem razgovoru omenila, da si je na telefon namestila aplikacijo AnyDesk.

Glede na to, kar je navedeno v prejšnjem odstavku, posrednik v tem nezavezujočem mnenju izhaja iz predpostavke, da so bile transakcije avtentificirane in da so bili osebam, ki so odobrile sporna plačila, poznani vsi osebni podatki, brez katerih teh transakcij ne bi bilo mogoče izvesti, do njih pa so prišli s pomočjo aplikacije AnyDesk, ki jim je omogočila oddaljen dostop in prevzem nadzora nad pobudničinim telefonom.

V tem primeru gre torej za neodobrene transakcije, saj jih ni odobrila pobudnica. Banka načeloma odgovarja za neodobrene transakcije, svoje (objektivne, ne glede na krivdo) odgovornosti pa se lahko reši, kadar je izvršitev transakcije posledica uporabnikove prevare ali goljufije ali če je uporabnik ravnal naklepno ali zaradi hude malomarnosti (tretji odstavek 137. člena ZPlaSSIED).

Za odločitev o tem, kdo naj nosi škodo, nastalo zaradi transakcij, opravljenih v nasprotju s pobudničino voljo, je zato treba odgovoriti na vprašanje, ali je pobudnica kršila pogoje, ki urejajo uporabo plačilnega instrumenta, in pri tem ravnala s hudo malomarnostjo.

S tem, ko je omogočila, da je nekdo tretji z uporabo aplikacije AnyDesk lahko prevzel nadzor



nad njenim telefonom, s tem pa tudi do pobudničine mobilne banke, je pobudnica kršila obveznost, ki ji jo v zvezi s plačilnimi instrumenti in osebnimi varnostnimi elementi nalaga določba 132. člena ZPlaSSIED. Ta določa, da uporabnik uporablja plačilni instrument v skladu s pogoji, ki urejajo izdajo in uporabo plačilnega instrumenta ... ter takoj po prejemu plačilnega instrumenta zlasti zagotovi vse razumne ukrepe, da zavaruje osebne varnostne elemente plačilnega instrumenta. Podobne določbe imajo tudi splošni pogoji banke.

Vprašanje je, ali je pobudnica pri tem ravnala hudo malomarno. Hudo malomarnost predstavlja ravnanje, pri katerem oseba ravna z manjšo skrbnostjo od skrbnosti, ki se v posameznem primeru pričakuje od vsakega razumnega človeka. Kaj se pričakuje od vsakega razumnega človeka, pa se presoja upoštevajoč okoliščine posameznega primera. Po mnenju posrednika v sporu ravnanje, ko nekdo omogoči neznani osebi oddaljen dostop do njegove spletne banke, odstopa od ravnanja vsakega razumnega uporabnika bančnih storitev in zato ravna s hudo malomarnostjo. V času, ko je opozarjanje na spletne prevare v javnih medijih in preko pogostih opozoril bank izjemno obsežno, je razumno pričakovati, da so uporabniki bančnih storitev s tem dobro seznanjeni, zato je že od manj skrbnega uporabnika mogoče pričakovati, da neznancu ne bo omogočil takega oddaljenega dostopa. Poleg tega ni mogoče prezreti, da je banka pobudnico s sms sporočilom opozorila, da je bilo njeno geslo v Rekono aplikaciji spremenjeno in naj ji sporoči, če spremembe ni opravila ona, a se pobudnica na opozorilo ni odzvala. Banka torej za obravnavane finančne transakcije ne more biti odgovorna.

Mnenje v sporu zaradi neodobrenih transakcij – 18.2.2025

Pobudnik zatrjuje, da je bil žrtev spletne prevare. Na spletni trgovini je kupil izdelek, ki naj bi ga plačal po povzetju, prav z razlogom, da ne bo ogoljufan. Trgovec mu je po SMS sporočil, da je blago predano Pošti Slovenija. Naslednji dan mu je Pošta Slovenija po SMS sporočila, da so podatki naslovnika pomanjkljivi. Dodana je bila spletna stran, na kateri naj bi popravil podatke (Ivandol je pošta Leskovec in ne Krško). Istočasno pa je bilo zahtevano plačilo dodatnega stroška 75 centov ali pa se pošiljka vrne prodajalcu. Takoj je reagiral in nakazal znesek. Trenutek zatem je prejel SMS Addiko banke o plačilu in to 630,36 na Booking. Tisti trenutek sploh ni vedel, za kaj gre. Poklical je hči, ki mu je povedala, da so posredi hekerji in naj nemudoma pokliče poslovalnico banke v Krškem. Bančna uslužbenka mu je svetovala, da takoj prekliče kartico in se zgloži v poslovalnici, da se naredi zapisnik. Pobudnik (tedaj kot pritožnik) je v pritožbenem obrazcu označil, da navedene transakcije ni opravil, niti ni nikogar pooblastil, da opravi nakup namesto njega. Kartice ni izgubil, niti mu ni bila ukradena, ves čas jo je imel pri sebi.

Pobudnik dodaja, da se na izpisku poslovanja po kartici vidi izplačilo v valuti. Zato je jasno, da plačila na Booking ni izvedel sam. Ker je upokojenec, je zanj to hud finančni udarec.

Banka, ki zavrača zahtevek pobudnika, v odgovoru pojasnjuje, da je šlo pri transakciji za zavarovano spletno transakcijo. Za transakcijo je avtentikacijo izvedel pritožnik sam v Rekono OnePass aplikaciji. Pritožnik je bil o transakciji obveščen z SMS sporočilom na svojo telefonsko številko. Kot je razvidno iz priložene slike zaslona iz avtorizacijskega sistema, je pritožnik transakcijo uspešno potrdil dne 30. 9. 2024 ob 12:47. Iz navedenega izhaja, da pritožnik ni postopal vsaj kot povprečno skrbna oseba, saj se od povprečno skrbne osebe pričakuje, da ne izvaja transakcij, v kolikor pred izvedbo transakcije ne preveri, ali bo denarna sredstva prejela upravičena oseba.

Iz dokumentacije in podatkov, vezanih na sporno transakcijo, po mnenju banke izhaja, da je



mogoče v obravnavanem primeru pritožniku očitati, da ni postopal v skladu z določili Splošnih pogojev poslovanja z Addiko kartico Mastercard (v nadaljevanju: Splošni pogoji) glede varovanja kartice pred zlorabo ter da je ravnal s hudo malomarnostjo, v posledici katere je prišlo do zlorabe njegove Mastercard kartice ter oškodovanja v skupnem znesku 630,36 EUR (oziroma 5.454,00 HKD).

Splošni pogoji v poglavju »Izguba, kraja ali zloraba kartice« določajo, da uporabnik v primeru neodobrene plačilne transakcije, ki bi nastala zaradi prevare, naklepa ali hude malomarnosti uporabnika, le-ta krije vso škodo. Enako določa tudi 3. odstavek 137. člena Zakona o plačilnih storitvah, storitvah izdaje elektronskega denarja in plačilnih sistemih (ZPlaSSIED), ki določa, da uporabnik krije celotno izgubo zneskov iz drugega in tretjega odstavka prejšnjega člena (tj. znesek neodobrene plačilne transakcije in v zvezi s transakcijo zaračunanimi nadomestili), če je izvršitev neodobrene plačilne transakcije posledica uporabnikove prevare ali goljufije, ali če uporabnik naklepno ali zaradi hude malomarnosti ni izpolnil ene ali več obveznosti v zvezi s plačilnim instrumentom v skladu s 132. členom navedenega zakona (tj. obveznost uporabnika plačilni instrument uporabljati v skladu s pogoji, ki urejajo izdajo in uporabo plačilnega instrumenta, zlasti zagotovitev vseh razumnih ukrepov za zavarovanje osebnih varnostnih elementov plačilnega instrumenta).

V skladu s Splošnimi pogoji se od uporabnika glede izpolnjevanja obveznosti v zvezi z uporabo plačilnega instrumenta, tj. Mastercard kartice, zahteva, da:

- mora uporabnik kartico skrbno hraniti in ravnati z njo kot dobre gospodar, in sicer tako da prepreči izgubo, krajo ali nepooblaščen uporabo kartice in vpogled v PIN (poglavje »Uporaba kartice« str. 3);
- se lahko uporabnik o varni uporabi kartic, varnem spletnem nakupovanju in zaščiti mobilne naprave pouči s pomočjo objav na spletni strani banke addiko.si (Varna uporaba kartic; Priporočila za varno internetno poslovanje).

Za banko je ključno, da pobudnik ni izvedel nobene transakcije v višini 0,75EUR, pač pa je izvedel avtentikacijo v Rekono OnePass aplikaciji za znesek 630,36 EUR. V kolikor bi pobudnik ravnal z vso skrbnostjo, transakcije ne bi potrdil v Rekono OnePass aplikaciji, saj je pri potrditvi razvidna višina transakcije, ki se potrjuje, prav tako je razvidno prodajno mesto za katero se potrjuje transakcija in torej se ni izpisalo »Pošta Slovenije« temveč »Booking.comAttr«.

Glede spletnih prevar je banka stranke večkrat opozarjala in jih hkrati pozvala k večji pazljivosti. Prav tako je banka stranke opozarjala o zlorabah in s tem v zvezi v spletni banki ter na spletnih strani banke objavila opozorilna obvestila. Nenazadnje pa tudi Splošni pogoji napotujejo na vsebine glede varne uporabe plačilnih kartic ter pogostih načinov spletnih zlorab, s katerimi je priporočljivo, da se uporabniki kartic seznani in s tem pripomorejo k preprečevanju zlorab.

Ker med pobudnikom in banko ni bil dosežen sporazum o rešitvi spora, izdaja posrednik v sporu na podlagi določbe drugega odstavka 14. člena Pravil postopka za izvensodno reševanje potrošniških sporov pri Združenju bank Slovenije naslednje

nezavezujoče mnenje o spornem razmerju:

Pobuda je utemeljena.

Če uporabnik plačilne storitve, tako kot v tem primeru pobudnik, trdi, da ni odobril izvršene plačilne transakcije, zgolj uporaba plačilnega instrumenta, ki jo evidentira (v tem primeru)



banka, po določbi 3, odstavek 148. člena ZPlaSSIED ni nujno zadosten dokaz, da je plačnik odobril plačilno transakcijo ali da je goljufal ali da naklepno ali iz hude malomarnosti ni izpolnil ene ali več obveznosti iz 132. člena istega zakona. Banka mora zagotovi dokaze, da je uporabnik plačilne storitve ravnal goljufivo, s prevaro ali hudo malomarno.

Banka ne nasprotuje trditvi pobudnika, da je bil žrtev spletne prevare. Za žrtev spletne prevare ni mogoče trditi, da je odobrila plačilno transakcijo. Pobudnik je verjel, da plačuje Pošti Slovenije znesek 0,75 EUR, dejansko pa je plačal 630,36 EUR na „Booking.comAttr“. Kljub avtentikaciji ni šlo za odobreno plačilo.

Banka se pravilno sklicuje na določbo 3. odstavek 137. člena ZPlaSSIED, po kateri uporabnik krije znesek neodobrene plačilne transakcije in v zvezi s transakcijo zaračunanimi nadomestili, če je izvršitev neodobrene plačilne transakcije posledica uporabnikove prevare ali goljufije, ali če uporabnik naklepno ali zaradi hude malomarnosti ni izpolnil ene ali več obveznosti v zvezi s plačilnim instrumentom v skladu s 132. členom ZPlaSSIED (tj. obveznost uporabnika plačilni instrument uporabljati v skladu s pogoji, ki urejajo izdajo in uporabo plačilnega instrumenta, zlasti zagotovitev vseh razumnih ukrepov za zavarovanje osebnih varnostnih elementov plačilnega instrumenta).

Po povedanem je ključno vprašanje v tej zadevi, ali je pobudniku mogoče očitati hudo malomarnost, ko je potrdil napačno plačilo. Gotovo ni bil dovolj pozoren pri potrjevanju transakcije, a premajhna pozornost še ne pomeni hude malomarnosti. Hudo malomarno je ravnanje, ki je skrajno nepazljivo in ne že tako, ki odstopa od ravnanja povprečno skrbne osebe, kot zmotno meni banka.

Seveda se od vsakogar pričakuje, da preveri, ali nakazuje pravi znesek pravi osebi. Vendar pa je treba pri presoji skrbnosti upoštevati konkretne okoliščine vsakega primera, pa tudi osebne lastnosti tistega, čigar ravnanje se presoja. Pobudnik je pričakoval pošto pošiljko in je prejel SMS sporočilo, ki je bilo po videzu od Pošte Slovenija. Ker je bila v njegovem naslovu res pomanjkljivost, očitana v SMS sporočilu, se ni zdelo povsem nesmiselno, da nekdo terja popravek. Na priloženi obrazec gotovo ni sam vpisal zneska 630,36 EUR, glede na potek predhodnega dogajanja pa je bil prepričan, da znesek 0,75 EUR nakazuje Pošti Slovenija. Ker je pobudnik starejša oseba (upokojenec), mora biti tudi kriterij za presojo hude nepazljivosti nekoliko milejši.

Banka se sklicuje na svoja opozorila pred spletnimi prevarami. Ta gotovo ozaveščajo uporabnike plačilnih instrumentov in s tem znižujejo prag, nad katerim neskrbno ravnanje postaja ne le malomarno, pač pa lahko preide v hudo malomarno ravnanje. Vendar pa splošna (in pogosto dolgovezna) brezčasna opozorila na spletne prevare ne morejo imeti enakega učinka kot konkretna opozorila, npr. da se prevaranti v zadnjem času poslužujejo logotipov znanih podjetij, npr. Pošte Slovenije z dodanim opisom najpogostejših načinov prevar. Da bi pa pobudnik prejel tako opozorilo, pa ni izkazano.

Po zgoraj povedanem je bilo pobudnikovo ravnanje sicer malomarno, a ni doseglo stopnje hude malomarnosti. Zato niso izpolnjeni pogoji, da sam krije izgubo zaradi sporne plačilne transakcije po določbi 3. odstavek 137. člena ZPlaSSIED.

Mnenje v sporu zaradi neodobrenih transakcij – 25.2.2025

Pobudnica je v pobudi, ki jo je vložila njena hči kot pooblaščenka, navedla, da je bila 12. 7. 2024



žrtev spletne goljufije. Ker ni vedela, da je prevarantom omogočila dostop do spletne banke, so ji izpraznili osebni račun, varčevalni račun, povečali limit in vzeli hitri kredit ter izpraznili tudi hčerkin račun, na katerem je bila pooblaščenca. Ves ta denar, ki je bil v kratkem času zbran na pobudničinem bančnem računu, je šel v nakup kripto valut v 25 transakcijah. Transakcije so se začele ob 17:49, kreditna pogodba je bila sklenjena ob 18:30, izredni limit ob 18:31, nato pa so se transakcije nadaljevale. Bankin algoritem je po trditvah pobudnice zaznal anomalijo šele nekaj pred 20:00 uro. Pobudnica ni nikoli poslovala s tako velikimi zneski, zato bi banka morala prej zaznati, da je nekaj narobe. Pobudnica je bila že takrat v trajnem bolniškem staležu, leta 2025 pa bi se morala upokojiti. Oba njena dohodka nista dovolj za preživetje po odtrganem obroku kredita. Pobudnica je prosila banko za pomoč, če bi se lahko dogovorila vsaj za oprostitev stroškov in obresti kredita ter dela kredita.

Banka je v odgovoru na pobudo navedla, da iz policijskega zapisnika izhaja, da je pobudnica 12. 7. 2024 okrog 11:00 ure videla na Facebooku oglas, da vračajo denar oškodovancem. Ker je bila sama pred leti oškodovana, se je odločila, da jih kontaktira. Nato je prejela telefonski klic neznanega moškega, ki ji je povedal, da bo denar dobila nazaj. Neznanec ji je dal navodila za namestitve aplikacij Supremo in Binance, nato pa je po njegovih navodilih odprla aplikacijo in vnesla številko kartice. Do zlorabe je torej po stališču banke prišlo zato, ker je pobudnica neznanim osebam omogočila oddaljen dostop do svoje naprave, s tem pa so pridobili tudi dostop do njenih osebnih/kartičnih podatkov in e-banke. Ko so vstopili v e-banko, so najeli kredit 40.000,00 EUR, pri čemer so nastali še stroški, najeli izredni limit, pri čemer so prav tako nastali stroški, izvedli prenos zneska 6.200,00 EUR z računa hčere, prenos z varčevalnega računa 1.900,00 EUR, končno pa izvedli 25 kartičnih plačil po 2.500,00 EUR, skupno torej 62.500,00 EUR v roku približno 2 ur. Banka poudarja, da so pobudnico ob 19:48 uri klicali, ker so želeli zvedeti, ali sama opravlja transakcije; potrdila je, da transakcije nakupa kripto valut opravlja sama in šele po dodatnih vprašanjih in poizvedovanju agentke se je končno zavedala, da gre najverjetneje za goljufijo, zato so v banki izvedli vse potrebne blokacije.

Banka je navedla še, da so bile vse transakcije, ki jim pobudnica oporeka, izvedene in potrjene v elektronski denarnici pobudnice NLB Pay. Pobudnici je želela pomagati in prodajnemu mestu v sodelovanju s procesnim centrom Bankart d.o.o. poslati finančne reklamacije. Žal pa to ni bilo mogoče, saj so bile transakcije potrjene v elektronski denarnici NLB Pay.

Na koncu banka opozarja, da je bilo pobudnici na njeno telefonsko številko že za prvo transakcijo v višini 2.500,00 EUR poslano SMS sporočilo, da so na njeni kartici zaznali transakcijo SPLETNI NAKUP Bifinity Deposit in da so kartici omejili poslovanje; pozvali so jo, naj v primeru, da je nakup opravila sama, odgovori POTRDI in kodo 78. Pobudnica je banki SMS s potrditveno kodo tudi poslala in s tem potrdila, da plačilo res izvaja ona sama.

Glede na to je banka mnenja, da je pobudnica ravnala v nasprotju z določbami 132. člena Zakona o plačilnih storitvah, storitvah izdajanja elektronskega denarja in plačilnih sistemih (ZPlaSSIED, Uradni list RS, št. 7/18, 9/18 – popr. in 102/20). Banka meni, da je pobudnica ravnala s hudo malomarnostjo, zaradi česar je sama odgovorna za celotno izgubo zneskov skladno z določbo tretjega odstavka 137. člena ZPlaSSIED.

Na naroku dne 13. 12. 2024 je pooblaščenec pobudnice vložil novo vlogo, ki je bila vročena pooblaščenkam banke, narok pa je bil preložen, da je banka lahko odgovorila na navedbe v tej vlogi. V njej je pooblaščenec pobudnice opozoril, da iz odgovora banke na pobudo izhaja, da je bilo v pobudničino e-banko ob 18:00:52 uri hkrati dostopano preko dveh IP naslovov, ki se nahajata na različnih lokacijah, zato je najmanj takrat obstajal sum, da je prišlo do resne anomalije, kar banki ni moglo ostati neznano. Navedel je še, da banka ni ravnala v skladu z ZPPDFT-2, ker ni opravila pregleda stranke pri transakciji, večji od 15.000,00 EUR. Če bi preverila stanje, bi banka vedela, da je pobudnica prodajalka, da se ni nikoli ukvarjala z nakupom kriptovalut, da ni potrebovala kredita in izrednega limita, kar utemeljuje sum kaznivega dejanja, katerega izvajanje bi morala



banka preprečiti. Po mnenju pobudničnega pooblaščenca je šlo v tem primeru tudi za sum pranja denarja.

Banka je na navedbe iz omenjene vloge odgovorila, da je opravila pregled stranke po ZPPDFT-2 ob sklenitvi poslovnega razmerja s pobudnico, v obravnavanem primeru pa ji ga ni bilo treba opraviti ponovno, saj ni šlo za nova poslovna razmerja, ampak za posle v okviru že obstoječega razmerja med njo in pobudnico.

V novi vlogi z dne 17. 1. 2025 je pooblaščenec pobudnice še bolj natančno in obširno utemeljeval, zakaj je v tem primeru prišlo do kršenja ZPPDFT-1 in zakaj so bile transakcije, s katerimi je bila oškodovana pobudnica, zelo nenavadne in sumljive z vidika pranja denarja.

Banka je v odgovoru na to vlogo ponovila, da je pravilno izvajala vse ukrepe po ZPPDFT-1. Ponovno je poudarila, da je že ob prvi zaznani transakciji poslala pobudnici opozorilo s pozivom, naj pošlje potrditveni SMS, če transakcijo izvaja sama, kar je pobudnica tudi storila. Banka trdi tudi to, da zgolj različni IP naslovi ne predstavljajo faktorja, zaradi katerega bi bila transakcija sumljiva, saj je namen spletnih bank ravno v tem, da lahko stranke dostopajo do njih s kateregakoli IP naslova, pri čemer pa je bistveno, da so aplikacije in spletne banke zavarovane s standardi močne avtentikacije strank.

Na naroku 20. 1. 2025 do sporazuma med pobudnico in banko ni prišlo. Zato je posrednik v sporu na podlagi določbe drugega odstavka 14. člena Pravil postopka za izvensodno reševanje potrošniških sporov pri ZBS (v nadaljevanju: Pravila) izdal to nezavezujoče mnenje.

Pobuda je delno utemeljena.

V tej zadevi ni sporno, da je pobudnica 12. 7. 2024 sama navezala stik z neznancem, za katerega je mislila, da ji bo pomagal priti nazaj do denarja, za katerega je bila ogoljufana pred 5 do 6 leti. Na njegovo zahtevo je naložila na svojo napravo aplikaciji Supremo in Binance ter odprla e-banko. Z namestitvijo aplikacije Supremo je neznancu omogočila oddaljen dostop do svoje naprave, s tem do svoje spletne banke, v kateri je neznanec nato izvedel vse obravnavane finančne transakcije. Te transakcije so neodobrene, saj jih ni odobrila pobudnica. Banka načeloma odgovarja za neodobrene transakcije, svoje (objektivne, ne glede na krivdo) odgovornosti pa se lahko reši, kadar je izvršitev transakcije posledica uporabnikove prevare ali goljufije ali če je uporabnik ravnal naklepno ali zaradi hude malomarnosti (tretji odstavek 137. člena ZPlaSSIED).

Za odločitev o tem, kdo naj nosi škodo, nastalo zaradi transakcij, opravljenih v nasprotju s pobudničino voljo, je zato treba odgovoriti na vprašanje, ali je pobudnica kršila pogoje, ki urejajo uporabo plačilnega instrumenta, in pri tem ravnala s hudo malomarnostjo.

S tem, ko je omogočila, da je nekdo tretji z uporabo aplikacije Supremo lahko prevzel nadzor nad njeno napravo, s tem pa tudi pridobil dostop do njene spletne banke, je pobudnica kršila obveznost, ki ji jo v zvezi s plačilnimi instrumenti in osebnimi varnostnimi elementi nalaga določba 132. člena ZPlaSSIED. Ta določa, da uporabnik uporablja plačilni instrument v skladu s pogoji, ki urejajo izdajo in uporabo plačilnega instrumenta ... ter takoj po prejemu plačilnega instrumenta zlasti zagotovi vse razumne ukrepe, da zavaruje osebne varnostne elemente plačilnega instrumenta.

Vprašanje je, ali je pobudnica pri tem ravnala hudo malomarno. Hudo malomarnost predstavlja ravnanje, pri katerem oseba ravna z manjšo skrbnostjo od skrbnosti, ki se v posameznem primeru pričakuje od vsakega razumnega človeka. Kaj se pričakuje od vsakega razumnega človeka, pa se presoja upoštevajoč okoliščine posameznega primera. Po mnenju posrednika v sporu ravnanje, ko nekdo omogoči neznanu osebi oddaljen dostop do njegove spletne banke, odstopa od ravnanja vsakega razumnega uporabnika bančnih storitev in zato ravna s hudo malomarnostjo. V času, ko je opozarjanje na spletne prevare v javnih medijih in preko pogostih opozoril bank izjemno obsežno, je razumno pričakovati, da so uporabniki bančnih storitev s tem dobro seznanjeni, zato



je že od manj skrbnega uporabnika mogoče pričakovati, da neznancu ne bo omogočil takega oddaljenega dostopa.

Poleg tega ni mogoče prezreti, da je banka pobudnici že ob prvi zaznani transakciji, še pred začetkom zlorabe, na njeno telefonsko številko poslala SMS-notifikacijo, da je zaznala spletno transakcijo v višini 2.500,00 EUR in zaradi varnosti omejila poslovanje s kartico. Pozvala jo je, naj v primeru avtorizacije transakcije pošlje povratni SMS z vsebino POTRDI 78. Njen potrditveni SMS z navedeno vsebino je banka tudi prejela, nakar so stekle transakcije po 2.500,00 EUR. Te bankine navedbe pobudnica niti ne zanika in jo posrednik v sporu zato šteje za resnično. Načeloma torej banka ne bi mogla biti odgovorna za obravnavane transakcije.

Vendar pa posrednik v sporu ugotavlja, da obstajajo okoliščine, v katerih bi banka lahko zmanjšala škodo, nastalo pobudnici. Pri tem posrednik nima v mislih obveznosti banke v zvezi s predpisi o preprečevanju pranja denarja in financiranja terorizma. Pač pa opozarja na dejstvo, da je bilo opravljenih s pobudničinega računa v kratkem času kar 25 transakcij po 2.500,00 EUR, poleg tega pa sta bila vzeta še hitri kredit in izredni limit, prišlo je do prenosa denarja s pobudničinega varčevalnega računa in računa njene hčere na njen osebni račun. Glede na pobudničin finančni položaj posrednik v sporu ne dvomi, da je bilo tako poslovanje izrazito v nasprotju s pobudničnim običajnim poslovanjem, kar bi banka gotovo lahko ugotovila. Res je sicer, da je že ob prvi transakciji v znesku 2.500,00 EUR opozorila pobudnico, da je transakcija sumljiva in jo pozvala, naj jo posebej potrdi, kar je pobudnica tudi storila. Ravno to, da je bila banki sumljiva že prva transakcija, pa po mnenju posrednika kaže, da bi morala banka še naprej bolj pazljivo spremljati, kaj se je dogajalo in pobudnico bistveno prej kot ob 19:48 uri, ko je bilo izvršenih že vseh 25 transakcij, poklicati in jo izrecno opozoriti na sumljivo dogajanje. Ob tem ni nezanemarljivo tudi dejstvo, da je bilo tistega dne opravljenih več vstopov v pobudničino e-banko in to z dveh različnih IP naslovov, ki sta na različnih lokacijah, pri čemer sta bila ob isti uri (18:00:52) opravljena vstopa hkrati iz obeh lokacij. Pobudnik sicer sprejema trditev banke, da je možnost dostopanja do spletne banke z več naslovov in z različnimi napravami ena od bistvenih lastnosti spletnega bančništva in samo po sebi s tem ni nič narobe. Pač pa je v okoliščinah tega primera tudi to dejstvo tako, da bi moralo banki vzbuditi dodatno pozornost. Posrednik v sporu se ne opredeljuje, kje je tista meja oziroma tisti trenutek, ko bi morala banka reagirati in pobudnico (ponovno) opozoriti na nevarnost goljufije. Od banke pričakuje, da bo s pobudnico vendarle še enkrat skušala zadevo urediti s sporazumom in ji pri tem ponuditi nekaj več kot samo odpust vseh stroškov, povezanih s kreditom in izrednim limitom, pod pogojem, da pobudnica takoj poplača celoten kredit, kot ji je ponudila na naroku 20. 1. 2025.

Mnenje v sporu dvig na bankomatu – 25.2.2025

Pobudnica navaja, da je dne 20. 9. 2024 na bankomatu v Europarku v Mariboru hotela dvigniti 100,00 EUR. Po končanem vnosu pin-a in zneska ji bankomat denarja ni izplačal. Nato je dvig uspešno opravila na drugem bankomatu. Njena reklamacija pri banki je bila zavrnjena, češ da je bil denar izplačan, na bankomatu pa niso zaznali težav. Reklamacije ne bi vložila, če bi ji bil denar izplačan.

Banka nasprotuje pobudničini zahtevi. Navaja, da je opravila pregled bankomata in pridobila mnenje Bankarta, iz katerega izhaja, da je bila reklamirana transakcija na bankomatu odobrena in izplačana. Natančno opisuje potek dogodkov na bankomatu in trdi, da je iz dnevnika bankomata razvidno, da so na njem tistega dne brez posebnosti zavedene predhodne in kasnejše transakcije drugih uporabnikov bankomata. Ob prevzemu gotovine pri praznitvi bankomata in ponovnem polnjenju dne 30. 9. 2024 pa ni bil ugotovljen presežek gotovine. Priložila je še mnenje procesnega centra Bankart, ki pritruje banki, da je bankomat



izplačal zahtevni znesek.

Pobudnica na narok 20. 1. 2025 ni prišla, zato ga je posrednik v sporu skladno z določbo prvega odstavka 13. člena Pravil postopka za izvensodno reševanje potrošniških sporov pri ZBS (v nadaljevanju Pravila) opravil brez njene udeležbe. Že zaradi odsotnosti pobudnice sporazuma med njo in banko ni bilo mogoče doseči, zato je posrednik v sporu izdal to nezavezujoče mnenje (drugi odstavek 14. člena Pravil). Z dnem, ko bo pobudnica z njim seznanjena, se skladno z določbo 3. alineje tretjega odstavka 14. člena Pravil šteje, da je postopek v tej zadevi končan.

Pobuda ni utemeljena.

Po določbi prvega odstavka 148. člena Zakona o plačilnih storitvah, storitvah izdajanja elektronskega denarja in plačilnih sistemih (ZPlaSSIED, Uradni list RS, št. 7/18, 9/18 – popr. in 102/20) mora ponudnik plačilnih storitev (banka) v primeru, ko uporabnik trdi, da plačilna transakcija ni bila izvršena pravilno, dokazati, da je bila plačilna transakcija pravilno evidentirana ter da na njeno izvršitev ni vplivala nikakršna tehnična okvara ali druga pomanjkljivost storitve, ki jo je opravil uporabnik.

Banka je v tej zadevi zelo prepričljivo opisala in z dokazi podprla svoje ugotovitve, da je bankomat, na katerem je pobudnica dvigovala gotovino, tistega dne delal brez napak. To je ugotovila banka sama, njene ugotovitve pa je podprl tudi procesni center Bankart. Iz zapisov dnevnika bankomata tako sledi ves postopek, ki ga je opravila pobudnica – točen čas vstavitve kartice in avtorizacije transakcije, prevzema kartice iz reže čitalca, izplačila gotovine (v apoenu 100,00 EUR) ter prevzema bankovca iz reže bankomata za izdajo gotovine. Tudi ob štetju gotovine ob prvi praznitvi bankomata po dnevu, ko ga je uporabila pobudnica, v njem ni bilo presežka denarja, ki bi se moral pokazati, če bankomat pobudnici ne bi izplačal zahtevanih 100,00 EUR. Posrednik v sporu tako meni, da je banka izpolnila dokazno breme iz prvega odstavka 148. člena ZPlaSSIED, zato je pobudnična pobuda neutemeljena.

Mnenje v sporu zaradi izbrisa datoteke – 25.2.2025

Pobudnica je v pobudi navedla, da je prodala garažo, na kateri ima banka vknjiženo hipoteko v zavarovanje njene kreditne obveznosti. Namen prodaje je bil, da s kupnino stabilizira svoje finance in nadaljuje z dobrim poslovanjem. Vendar pa banka ni hotela ugoditi njeni prošnji za izbris hipoteke ter izdajo izbrisne pobotnice in je to pogojevala s tem, da pobudnica celotno kupnino usmeri v poplačilo kredita. Pobudnica meni, da je tak pogoj neutemeljen, ker je nesorazmeren, predvsem zato, ker je njena obveznost v znesku 120.000,00 EUR dovolj zavarovana s hipoteko na njenem stanovanju, vrednem 254.000,00 EUR. Nezadovoljna je tudi zato, ker banka na njeno prošnjo ni odgovorila več kot štiri mesece. Od banke pričakuje, da ji povrne preostalo kupnino od garaže v višini 23.000,00 EUR ter plača odškodnino za škodo zaradi zamud in pogojev, ki ji jih je postavila.

Banka priznava, da je bil čas od prejema pobudnične vloge 2. 7. 2024 za delni izbris hipoteke do njenega odgovora 6. 11. 2024 nesorazmerno dolg. Za to se je pobudnici opravičila in jo v znak opravičila oprostila plačila vodenja njenega paketa Premium za 3 mesece. Glede vsebine spornega razmerja pa banka navaja, da glede na poslovanje pobudnice njena odločitev o delnem izbrisu hipoteke ne bi bila nič drugačna julija kot je bila novembra. Opisuje tudi, kako je po prejemu pobudničinega soglasja dne 19. 11. in 20. 11. 2024 porabila preostanek kupnine v višini 28.000,00 EUR, med drugim tudi za poplačilo kredita v višini 20.000,00 EUR, o čemer je s pobudnico sklenila aneks h kreditni pogodbi. Njene zahteve v celoti zavrača.



Na naroku sta pobudnica in banka vztrajali vsak pri svojih stališčih in sporazuma med njima ni bilo mogoče doseči. Zato je posrednik v sporu v skladu z določbo drugega odstavka 14. člena Pravil postopka za izvensodno reševanje potrošniških sporov pri ZBS izdal to nezavezujoče mnenje.

Pobuda ni utemeljena.

Iz navedb banke, ki jim pobudnica ne oporeka, sledi, da sta pobudnica in banka že pred začetkom tega postopka uredili sporno razmerje s tem, da je pobudnica soglašala, kako naj banka uporabi preostali del kupnine in glede odplačevanja kredita sklenili aneks h kreditni pogodbi. Ob tako veljavno urejenem pogodbenem razmerju med strankama so zato pobudnične zahteve, ki jih uveljavlja v tem postopku, neutemeljene. Pogodba namreč zavezuje stranki in bi jo stranki lahko spremenili samo soglasno. To bi se lahko zgodilo tudi v tem postopku izvensodnega reševanja spora, a se ni, ker banka ni pripravljena ugoditi zahtevam pobudnice. O veljavnosti ali neveljavnosti pogodbe pa posrednik v tem sporu ne more odločati. Pobudnica lahko tak zahtevek uveljavlja le v sodnem postopku.

Mnenje v sporu zaradi neodobrenih transakcij – 4.3.2025

Pobudnik je v pobudi navedel, da je podatke svoje plačilne kartice nehote vpisal v neko drugo Google denarnico, s katere so nato za več zneskov bremenili njegov račun. Po sedmem zaporednem nakupu so mu iz banke poslali SMS z vsebino: „Na kartici ****9251 smo zaznali sumljivo transakcijo POS NAKUP, 16.11.2024 18:15:36, IP SARSEEVA, 957,95 EUR. Če transakcije niste opravili vi, odgovorite v 180 minutah s ključno besedo STOP in unikatno kodo 70 (primer: STOP 70) in nadaljnje transakcije bodo onemogočene.“ Pobudnik trdi, da je na ta SMS odgovoril v nekaj minutah, a je banka kljub temu omogočila še 5 nadaljnjih transakcij v skupnem znesku 427,40 EUR, ki mu jih banka na njegov poziv ni hotela vrniti.

Banka v odgovoru na pobudo navaja, da je bila namestitev pobudnikove virtualne kartice v Google Denarnico potrjena dne 16. 11. 2024 ob 18:12:28 uri. Banka je takoj za tem pobudniku na njegovo telefonsko številko poslala SMS obvestilo z naslednjo vsebino: „Pozdravljeni, vazo kartico ****9251 ste uspešno dodali v GOOGLE PAY. Če je niste dodali vi, nemudoma poklicite na 01 583 41 83 in blokirajte vazo kartico.“ Po trditvah banke bi pobudnik lahko preprečil vse transakcije od blokade dalje, če bi po prejemu tega obvestila blokiral kartico, pa tega ni storil. Ko so se potem začele transakcije, je bil pobudnik o vsaki od njih obveščen s SMS sporočilom na njegovo telefonsko številko. Po potrjeni sedmi transakciji je nato banka pobudniku poslala še SMS sporočilo, na katerega se sklicuje tudi pobudnik. Sporočilo je pobudnik prejel ob 18:19:00 uri, nanj odgovoril z odgovorom STOP 70 ob 18:20:59 uri in banka je takoj onemogočila nadaljnje transakcije. Banka trdi, da je bilo vseh 5 transakcij, za katere pobudnik zahteva vrnitev denarja, izvedenih še preden je pobudnik posredoval SMS sporočilo z odgovorom STOP 70.

Po stališču banke je treba v tem primeru izhajati iz določb Zakona o plačilnih storitvah, storitvah izdajanja elektronskega denarja in plačilnih sistemih (ZPlaSSIED), Uradni list RS, št. 7/18, 9/18 – popr. in 102/20) in veljavnih splošnih pogojev banke za poslovanje s potrošniki. Po določbi tretjega odstavka 137. člena ZPlaSSIED uporabnik krije celotno izgubo, če zaradi hude malomarnosti ni izpolnil obveznosti v zvezi s plačilnim instrumentom v skladu s 132. členom, ki določa, da uporabnik uporablja plačilni instrument v skladu s pogoji, ki urejajo izdajo in uporabo plačilnega instrumenta ter takoj po prejemu plačilnega instrumenta zagotovi vse razumne ukrepe, da zavaruje osebne varnostne elemente plačilnega instrumenta. Tega pobudnik po mnenju banke ni storil in je vpisal podatke o svoji kartici, ne da bi preveril, kam. Po mnenju banke je s tem ravnal z manjšo skrbnostjo, kot je pričakovano od povprečno skrbnega uporabnika plačilne kartice, kar pomeni hudo malomarnost. Banka zato zavrača svojo odgovornost. Dodaja še, da prav z namenom osveščanja



svojih strank preko različnih komunikacijskih kanalov svojim komitentom svetuje, kako se zavarovati pred zlorabami in prevarami.

Pobudnik na narok 20. 1. 2025 ni prišel in že iz tega razloga ni bilo mogoče niti poskusiti doseči sporazuma med njim in banko. Zato je posrednik v sporu na podlagi določbe drugega odstavka 14. člena Pravil postopka za izvensodno reševanje potrošniških sporov pri ZBS izdal to nezavezujoče mnenje.

Pobuda ni utemeljena.

Skladno s prvim odstavkom 136. člena ZPlaSSIED plačnikov ponudnik plačilnih storitev (banka) odgovarja za izvršitev plačilne transakcije brez plačnikovega soglasja (neodobrena plačilna transakcija). Svoje (objektivne, ne glede na krivdo) odgovornosti pa se banka lahko reši, kadar je izvršitev transakcije posledica uporabnikove prevare ali goljufije ali če je uporabnik ravnal naklepno ali zaradi hude malomarnosti (tretji odstavek 137. člena ZPlaSSIED).

Za odločitev o tem, kdo naj nosi škodo, nastalo zaradi transakcij, opravljenih v nasprotju s pobudnikovo voljo, je zato treba odgovoriti na vprašanje, ali je pobudnik kršil pogoje, ki urejajo uporabo plačilnega instrumenta, in pri tem ravnal s hudo malomarnostjo.

S tem, ko je omogočil, da je nekdo tretji prišel do njegovih osebnih podatkov in varovalnih elementov, je pobudnik kršil obveznost, ki mu jo v zvezi s plačilnimi instrumenti in osebnimi varnostnimi elementi nalaga določba 132. člena ZPlaSSIED. Ta določa, da uporabnik uporablja plačilni instrument v skladu s pogoji, ki urejajo izdajo in uporabo plačilnega instrumenta ter takoj po prejemu plačilnega instrumenta zlasti zagotovi vse razumne ukrepe, da zavaruje osebne varnostne elemente plačilnega instrumenta.

Vprašanje je, ali je pobudnik pri tem ravnal hudo malomarno. Hudo malomarnost predstavlja ravnanje, pri katerem oseba ravna z manjšo skrbnostjo od skrbnosti, ki se v posameznem primeru pričakuje od vsakega razumnega človeka. Kaj se pričakuje od vsakega razumnega človeka, pa se presoja upoštevajoč okoliščine posameznega primera. Po mnenju posrednika v sporu ravnanje, ko nekdo preko telefona ali kako drugače posreduje občutljive osebne podatke, ki omogočajo dostop do njegove bančne kartice, odstopa od ravnanja vsakega razumnega uporabnika bančnih storitev in zato ravna s hudo malomarnostjo. V času, ko je opozarjanje na spletne prevare v javnih medijih in preko pogostih opozoril bank izjemno obsežno, je razumno pričakovati, da so uporabniki bančnih storitev s tem dobro seznanjeni, zato je že od manj skrbnega uporabnika mogoče pričakovati, da varovalnih podatkov ne bo posredoval tretjim osebam.

Posrednik v sporu na koncu ugotavlja še to, da je po njegovi oceni banka storila vse potrebne ukrepe, da bi lahko pobudnik obravnavane transakcije preprečil. Predvsem ga je že takoj po namestitvi njegove kartice na tujo napravo pozvala, naj ji sporoči, ali jo je namestil on, pa pobudnik na njeno SMS sporočilo ni odgovoril. Po vsaki transakciji mu je o njej poslala obvestilo, po sedmi transakciji pa še opozorilo, da gre za sumljive transakcije in naj ji pošlje sporočilo s kodo STOP 70, če želi onemogočiti nadaljnje transakcije. Banka je takoj po prejemu tega sporočila nadaljnje transakcije tudi onemogočila, a je bilo tudi tistih pet transakcij, za katera pobudnik zahteva vračilo, takrat že izvedenih. Vse to izhaja iz podatkov, ki jih je posredniku dala na voljo banka, pobudnik pa na narok, na katerem bi lahko tem trditvam nasprotoval, sploh ni prišel. Banka torej za obravnavane finančne transakcije ne more biti odgovorna.