LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

SPRENDIMAS DĖL X. X. IR *SWEDBANK*, AB, GINČO NAGRINĖJIMO

2022 m. liepos 14 d. Nr. 429-305
Vilnius

Lietuvos bankas gavo X. X. (toliau – pareiškėjas) kreipimąsi, kuriuo prašoma išnagrinėti tarp pareiškėjo ir *Swedbank*, AB, (toliau – bankas) kilusį ginčą.

N u s t a t y t a:

2022 m. balandžio 19 d. 23:33:42 val. Lietuvos laiku pareiškėjo vardu atidarytoje sąskaitoje banke (toliau – Sąskaita) pareiškėjo vardu išduota debeto kortele *Debit Mastercard* (toliau – Kortelė) įvykdyta mokėjimo operacija, kurios suma 250 Eur (toliau – Operacija).

2022 m. balandžio 19 d. 23:37:04 val. banko automatinė monitoringo sistema apribojo Kortelės dalinį funkcionalumą – atsiskaitymus už prekes ir paslaugas (liko tik galimybė Kortele vykdyti grynųjų pinigų operacijas). 23:41:32 val. bankas apie Kortelei pritaikytus apribojimus informavo pareiškėją SMS pranešimu, išsiųstu paskutiniu bankui nurodytu pareiškėjo tel. numeriu, nurodydamas: „Gerb. Kliente, apribojome mokėjimo kortelę (*duomenys neskelbtini*) dėl įtartinos operacijos revolutie. Jei jos neatlikote, kortelę privalote blokuoti, o jei atlikote – panaikinkite apribojimus Interneto banke ar programėlėje keičiant kortelės funkcionalumo nustatymus arba paskambinę „Swedbank" mokėjimo kortelėje nurodytu tel. nr."[1].

2022 m. balandžio 19 d. 14:55:39 val., t. y. iki Operacijos Kortele Sąskaitoje inicijavimo pradžios, bankas pareiškėjui išsiuntė SMS pranešimą, informuojantį apie tuo metu vykdomo Kortelės pridėjimo prie el. piniginės *Apple Pay* įrenginyje ir *Apple Pay* mokėjimo metodo aktyvavimo kodą: „Jūsų kortelės pridėjimo prie Apple Pay patvirtinimo kodas yra (*duomenys neskelbtini*). Šis kodas galios 30 minučių."[2].

2022 m. balandžio 19 d. 23:43:36 val. pareiškėjas banko interneto banko aplinkoje blokavo Kortelę.

2022 m. balandžio 19 d. 23:48:40 val. pareiškėjas parašė bankui interneto banko žinutę, kurioje nurodė, kad pastebėjo Sąskaitoje rezervuotą sumą Operacijai įvykdyti, ir pasiteiravo, ar galima Operaciją atšaukti.

2022 m. balandžio 20 d. 08:20 val. pareiškėjas kreipėsi telefonu į banką ir banko darbuotoja visam laikui blokavo Kortelę be galimybės ją atblokuoti. Pokalbio metu pareiškėjas nurodė, kad vakare pastebėjo ne jo įvykdytą Operaciją, o po to iškart gavo banko žinutę dėl Kortelės apribojimo ir pasiūlymo ją blokuoti, todėl iš karto blokavo Kortelę. Pareiškėjas taip pat nurodė, kad Sąskaitoje rezervuota 250 Eur suma. Darbuotojai pasiteiravus, ar negavo kažkokių pranešimų, el. laiškų ar pan., taip pat ar nepatvirtino, nesuvedė niekur Kortelės duomenų, pareiškėjas nurodė, kad gavo iš Lietuvos pašto pranešimą. Banko darbuotojai paklausus, ar buvo užsisakęs kažkokią pašto paslaugą, pareiškėjas nurodė, kad jam baigėsi kredito kortelės galiojimas, todėl jis pagalvojo, kad už atnaujintos kortelės atsiuntimą jo prašoma sumokėti 1,90 Eur sumą. Tuomet banko darbuotoja informavo pareiškėją, kad jis tapo sukčiavimo auka ir kad Operacijos nėra galimybės atšaukti. Taip pat pateikė informaciją, kad pokalbio metu užregistruos jo prašymą dėl Operacijos sumos grąžinimo tam, kad būtų galima įvertinti visas galimybes dėl Operacijos ginčijimo.

---

[1] Bankas atsiliepime nurodė, kad dėl Kortelės dalinio funkcionalumo apribojimo tą pačią dieną 23:34:38 val. ir 23:44:37 val. iki to laiko, kol pareiškėjas pateikė prašymą blokuoti Kortelę, tretiesiems asmenims nepavyko inicijuoti dar dviejų operacijų tam pačiam gavėjui.

[2] Bankas atsiliepime nurodė, kad 2022 m. balandžio 19 d. 14:55:40 val. bankas gavo informaciją, jog telekomunikacinių paslaugų teikėjas pristatė SMS pranešimą pareiškėjo tel. numeriu, nurodytu tiek Kortelės sutartyje, tiek ir pareiškėjo Lietuvos bankui adresuotame prašyme dėl vartojimo ginčo.

Pareiškėjas, informuotas apie banko sprendimą nekompensuoti jo nuostolių dėl Operacijos įvykdymo ir nesutikdamas su juo, kreipėsi į Lietuvos banką dėl ginčo nagrinėjimo. Kreipimesi pareiškėjas teigia, kad apgaulės būdu pavogus jo Kortelės duomenis buvo atliktas mokėjimas – Operacija, kuri pareiškėjui yra nežinoma, ir ją pareiškėjas teigia pastebėjęs tik patikrinęs banko mobiliosios programėlės pranešimą. Pareiškėjui nesuprantama, kodėl Operacijai įvykdyti nebuvo prašoma ją patvirtinti pareiškėjo turima tapatybės patvirtinimo priemone – *Smart-ID*. Kreipimesi pareiškėjas prašo rekomenduoti bankui grąžinti pareiškėjui jo ginčijamos Operacijos sumą – 250 Eur.

Bankas nesutinka keisti priimto sprendimo nekompensuoti pareiškėjo nuostolių dėl Operacijos įvykdymo. Bankas pažymi, kad pareiškėjo, kaip Kortelės naudotojo, tapatybė ginčijamų aplinkybių metu buvo nustatyta taikant sustiprintą mokėtojo tapatybės nustatymo procesą Kortelės pridėjimo kitame įrenginyje aktyvuojamo *Apple Pay* mokėjimo metodo metu. Tai yra buvo laikomasi saugesnio autentiškumo patvirtinimo reikalavimų naudojant technologijas, kuriomis galima užtikrinti saugų vartotojo autentiškumo patvirtinimą, – pareiškėjui asmeniškai atsiųstas vienkartinis kodas. Bankas pažymi, kad visos operacijos, kurių suma viršija 50 Eur, bekontakčiu būdu be papildomo mokėtojo autentifikavimo negali būti patvirtintos, tačiau pareiškėjo autentifikavimas Operacijos metu buvo atliekamas trečiųjų asmenų valdomame įrenginyje *Apple Pay* taikomomis sąlygomis, o Kortelės pridėjimas prie tame įrenginyje įdiegto *Apple Pay* atsiskaitymo būdo – panaudojant pareiškėjo iš banko asmeniškai gautą *Apple Pay* kodą. Banko vertinimu, akivaizdu, kad šiuo atveju pareiškėjas aktyviais veiksmais atskleidė šį kodą tretiesiems asmenims, nes be jo tretieji asmenys nebūtų galėję savo įrenginyje pridėti pareiškėjo Kortelės net ir tuo atveju, jei kitus Kortelės duomenis būtų gavę kitomis aplinkybėmis.

Bankas atkreipia dėmesį, kad pareiškėjas nesuabejojo gautame (trečiųjų asmenų siųstame) el. laiške nurodytu prašymu, nekreipė jokio dėmesio į tai, kad iš banko gavo *Apple Pay* aktyvavimo kodą, nors naudojasi *Android* įrenginiu, o šios aplinkybės galėjo ir turėjo atkreipti reikiamą pareiškėjo dėmesį. Banko manymu, gavęs iš banko SMS žinutę su *Apple Pay* kodu, pareiškėjas galėjo suprasti, kad šis kodas nėra skirtas sumokėti už siuntų tarnybos paslaugas, todėl turėjo susilaikyti nuo tolesnių veiksmų. Banko manymu, nuostolius dėl Operacijos pareiškėjas patyrė dėl savo didelio neatsargumo, perduodamas tretiesiems asmenims Kortelės duomenis (Kortelėje nurodytus savo vardą, pavardę, kortelės numerį ir CCV kodą) bei vienkartinį banko pareiškėjui nurodytu telefono numeriu siųstą Kortelės pridėjimo prie *Apple Pay* sistemos saugos kodą, ir taip suteikė leidimą tretiesiems asmenims pridėti Kortelę prie jų faktiškai valdomame įrenginyje įdiegto *Apple Pay* atsiskaitymo būdo. Tokiu būdu pareiškėjas suteikė galimybę Sąskaitoje vykdyti mokėjimo operacijas Kortele pareiškėjo vardu. Bankas prašo atmesti pareiškėjo reikalavimą kaip nepagrįstą.

K o n s t a t u o j a m a:

Vadovaujantis Lietuvos banko valdybos 2012 m. sausio 26 d. nutarimu Nr. 03-23 patvirtintų Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių 45 punktu, vartojimo ginčai Lietuvos banke nagrinėjami laikantis rungimosi, ginčų nagrinėjimo operatyvumo, koncentracijos, ekonomiškumo ir bendradarbiavimo principų. Vartotojas ir finansų rinkos dalyvis privalo įrodyti tas aplinkybes, kuriomis remiasi kaip savo reikalavimų arba atsikirtimų pagrindu, išskyrus atvejus, kai remiamasi aplinkybėmis, kurių nereikia įrodinėti. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Pareiškėjo ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjui pareiškėjo Kortele, panaudojant *Apple Pay* mokėjimo metodą, atliktos Operacijos, kurios vertė – 250 Eur ir kurios atlikti pareiškėjas teigia nedavęs sutikimo, sumą.

Pareiškėjas neigia autorizavęs Operaciją ir (arba) pridėjęs savo Kortelę prie *Apple Pay* sistemos naujame įrenginyje bei tvirtina, kad lėšos iš jo Kortelės sąskaitos buvo nurašytos dėl to, kad tretieji asmenys galėjo pasisavinti pareiškėjo Kortelės duomenis, todėl bankas turi grąžinti pareiškėjui Operacijos sumą. Atsiliepime bankas nurodo, kad Operacija bei kitos Sąskaitoje nepavykusios mokėjimo operacijos Kortele įvyko ne dėl sutrikimų banko ar tarptautinės mokėjimo kortelių organizacijos *Mastercard* sistemoje ar saugumo spragų jose, o dėl pareiškėjo veiksmų, kuriais tretiesiems asmenims buvo atskleisti pareiškėjo mokėjimo priemonių personalizuoti saugumo duomenys, dėl to tretieji asmenys įgijo galimybę savo įrenginiu inicijuoti mokėjimo operacijas pareiškėjo Sąskaitoje.

Mokėjimo paslaugų teikėjų veiklą ir atsakomybę, mokėjimo paslaugas, jų teikimo sąlygas ir informavimo apie šias sąlygas reikalavimus, mokėjimo operacijų autorizavimą ir

vykdymą, mokėjimo paslaugų vartotojų ir mokėjimo paslaugų teikėjų teises ir pareigas, susijusias su mokėjimo paslaugomis, kai mokėjimo paslaugų teikimas yra verslas, reglamentuoja Lietuvos Respublikos mokėjimų įstatymas.

Mokėjimų įstatymo 29 straipsnio 1 dalyje nustatyta, kad mokėjimo operacija laikoma autorizuota tik tada, kai mokėtojas duoda sutikimą įvykdyti mokėjimo operaciją. Jeigu mokėtojo sutikimo įvykdyti mokėjimo operaciją nėra, laikoma, kad mokėjimo operacija yra neautorizuota (Mokėjimų įstatymo 29 straipsnio 2 dalis).

Bankas atsiliepime nurodo, kad pareiškėjo ginčijama Operacija buvo atlikta naudojantis trečiųjų asmenų įrenginyje įdiegtu *Apple Pay* mokėjimo būdu, prie atitinkamo įrenginio, kuriame veikia *Apple Pay* sistema, pridėjus pareiškėjo Kortelę. Taigi, šalių neginčijamomis aplinkybėmis Operacija buvo inicijuota ir įvykdyta trečiųjų asmenų, jiems neteisėtu būdu sužinojus (pasisavinus) pareiškėjo mokėjimo priemonių personalizuotus saugumo duomenis ir juos panaudojus naujame įrenginyje pareiškėjo Kortelei pridėti prie *Apple Pay* sistemos, kuria pasinaudojant vėliau inicijuota ir įvykdyta pati Operacija. Akivaizdu, kad Operacijos inicijavimas ir patvirtinimas neatitiko paties pareiškėjo valios, nors formaliai (išoriniais požymiais) ir sutapo su pareiškėjo ir banko sutarta sutikimo mokėjimo operacijoms davimo forma ir tvarka. Pareiškėjo nurodytos aplinkybės, kad Operacija nėra pareiškėjo autorizuota, o pareiškėjo Kortelę prie *Apple Pay* sistemos naujame įrenginyje pridėjo ne pareiškėjas, o tretieji asmenys, bankas atsiliepime neginčija, todėl šio ginčo nagrinėjimo metu Lietuvos bankas daro išvadą, kad Operacija, atlikta nesant pareiškėjo valios ir jam net nežinant apie Operacijos inicijavimo aplinkybę bei neišreiškus jokių valinių veiksmų Operacijai patvirtinti, laikytina neautorizuota.

Dėl neautorizuotų mokėjimo operacijų pasekmių ir pareiškėjo teisės į Operacijos sumos grąžinimą

Pagal Mokėjimų įstatymo 38 straipsnio 1 dalį, mokėtojo mokėjimo paslaugų teikėjas privalo grąžinti mokėtojui neautorizuotos mokėjimo operacijos sumą ne vėliau kaip iki kitos darbo dienos nuo sužinojimo apie tokios mokėjimo operacijos įvykdymą, išskyrus atvejus, kai mokėtojo mokėjimo paslaugų teikėjas turi pagrįstų priežasčių įtarti mokėtojo sukčiavimą ir apie šias priežastis raštu praneša priežiūros institucijai (Lietuvos bankui).

Mokėjimų įstatymo 39 straipsnio 1 dalyje nustatyta, kad mokėtojui gali tekti dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai iki 50 Eur, kai šie nuostoliai patirti dėl 1) prarastos ar pavogtos mokėjimo priemonės panaudojimo; 2) neteisėto mokėjimo priemonės pasisavinimo. Tačiau, kaip nustatyta Mokėjimų įstatymo 39 straipsnio 2 dalyje, mokėtojas neturi patirti jokių nuostolių, jeigu 1) jis iki mokėjimo operacijos įvykdymo negalėjo pastebėti mokėjimo priemonės praradimo, vagystės arba neteisėto pasisavinimo, išskyrus atvejus, kai jis veikė nesąžiningai; 2) nuostoliai yra patirti dėl mokėjimo paslaugų teikėjo, jo darbuotojo, tarpininko, filialo ar asmenų, kuriems perduotas veiklos funkcijų valdymas, veiksmų ar neveikimo.

Mokėjimų įstatymo 39 straipsnio 3 dalyje nurodyta, kad „mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai, jeigu jis juos patyrė veikdamas nesąžiningai arba tyčia ar dėl didelio neatsargumo neįvykdęs vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų. Tokiais atvejais šio straipsnio 1 dalyje nustatytas didžiausios nuostolių sumos ribojimas netaikomas.“ Mokėjimų įstatymo 34 straipsnyje reglamentuojamos mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigos: 1) naudotis mokėjimo priemone pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas; 2) sužinojus apie mokėjimo priemonės praradimą, vagystę arba neteisėtą pasisavinimą ar neautorizuotą jos naudojimą, nedelsiant apie tai pranešti mokėjimo paslaugų teikėjui arba jo nurodytam subjektui. Mokėjimo paslaugų vartotojas, gavęs mokėjimo priemonę, privalo imtis veiksmų, kad būtų apsaugoti personalizuoti saugumo duomenys (Mokėjimų įstatymo 34 straipsnio 2 dalis).

Mokėjimų įstatymas aiškiai nustato, kad tuo atveju, kai mokėtojas neigia autorizavęs įvykdytą mokėjimo operaciją, mokėtojo mokėjimo paslaugų teikėjo arba atitinkamais atvejais mokėjimo inicijavimo paslaugos teikėjo užregistruotas mokėjimo priemonės naudojimas nebūtinai yra pakankamas įrodymas, kad mokėtojas autorizavo mokėjimo operaciją ar veikė nesąžiningai arba tyčia ar dėl didelio neatsargumo neįvykdė vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų. Mokėtojo mokėjimo paslaugų teikėjas ir atitinkamais atvejais mokėjimo inicijavimo paslaugos teikėjas turi pateikti įrodymų, kuriais patvirtinamas mokėtojo sukčiavimas arba didelis neatsargumas (Mokėjimų įstatymo 37 straipsnio 3 dalis).

Įvertinus pirmiau nurodytas Mokėjimų įstatymo nuostatas, galima teigti, kad mokėtojo

mokėjimo paslaugų teikėjas gali būti visiškai atleistas nuo pareigos grąžinti mokėtojui neautorizuotos mokėjimo operacijos sumą tik tuo atveju, jeigu pateikia įrodymų dėl mokėtojo sukčiavimo (nesąžiningumo arba tyčios) arba didelio neatsargumo (Mokėjimų įstatymo 37 straipsnio 3 dalis ir 39 straipsnio 3 dalis).

Aplinkybių ir duomenų, kaip ir šalių ginčo dėl to, kad pareiškėjas galėjo veikti nesąžiningai arba tyčia, įskaitant sukčiavimą, nėra. Tai reiškia, kad, siekiant įvertinti, ar bankas pagrįstai atsisako kompensuoti pareiškėjo nuostolius, susijusius su Operacijos įvykdymu, ir ar galėtų pareiškėjo atžvilgiu būti taikoma Mokėjimų įstatymo 39 straipsnio 3 dalis, būtina nustatyti, ar pareiškėjo elgesys, atskleidžiant tam tikrus personalizuotus mokėjimo priemonės (banko išduotos Kortelės) požymius, ir (arba) kiti veiksmai, dėl kurių galėjo būti įvykdyta Operacija, vertintini kaip didelis pareiškėjo neatsargumas, dėl kurio visi jo reikalaujami atlyginti nuostoliai turėtų tekti pačiam pareiškėjui.

Antrosios mokėjimo paslaugų direktyvos preambulės 72 punkte rašoma, kad „siekiant įvertinti galimą mokėjimo paslaugų vartotojo aplaidumą ar didelį aplaidumą, reikėtų atsižvelgti į visas aplinkybes. Įtariamo aplaidumo įrodymai ir laipsnis paprastai turėtų būti vertinami pagal nacionalinę teisę. Tačiau nors aplaidumo sąvoka reiškia, kad pažeidžiamas įsipareigojimas elgtis rūpestingai, didelis aplaidumas turėtų reikšti daugiau nei vien aplaidumą ir apimti labai nerūpestingą elgesį; pavyzdžiui, tai būtų mokėjimo operacijos autorizavimui naudojamų saugumo požymių laikymas prie mokėjimo priemonės atviru ir trečiosioms šalims lengvai atskleidžiamu formatu.“

Didelio neatsargumo sąvoka taip pat plėtojama ir Lietuvos Aukščiausiojo Teismo praktikoje. Kasacinis teismas yra išaiškinęs, kad „didelis neatsargumas kaip kaltės forma pasireiškia neprotingu arba išskirtiniu rūpestingumo nebuvimu, kai asmuo nėra tiek rūpestingas, kiek akivaizdžiai būtina esamomis aplinkybėmis“[3].

Bankas mano, kad nuostolius dėl Operacijos pareiškėjas patyrė dėl savo didelio neatsargumo, t. y. pareiškėjas, perduodamas tretiesiems asmenims savo Kortelės duomenis (Kortelėje nurodytus savo vardą, pavardę, kortelės numerį ir CCV kodą) bei vienkartinį banko pareiškėjui nurodytu telefono numeriu siųstą Kortelės pridėjimo prie *Apple Pay* sistemos saugos kodą, suteikė leidimą tretiesiems asmenims pridėti Kortelę prie jų faktiškai valdomame įrenginyje įdiegto *Apple Pay* atsiskaitymo būdo ir tokiu būdu suteikė galimybę tretiesiems asmenims Sąskaitoje vykdyti mokėjimo operacijas Kortele pareiškėjo vardu.

Vertinamų aplinkybių kontekste, visų pirma, būtina pažymėti, kad, remiantis pirmiau minėtų Mokėjimų įstatymo nuostatų analize, mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai tik tuo atveju, jei tenkinamos abi sąlygos, t. y. mokėtojas ne tik neįvykdo vienos ar kelių jam Mokėjimų įstatyme nustatytų pareigų, bet ir padaro tai elgdamasis nesąžiningai arba tyčia ar būdamas labai neatsargus. Taigi, banko sprendimas nekompensuoti pareiškėjo nuostolių dėl neautorizuotos Operacijos įvykdymo galėtų būti vertinamas kaip pagrįstas tik tuo atveju, jei būtų įrodyta, kad pareiškėjas, atskleisdamas tam tikrus personalizuotus savo mokėjimo priemonių saugumo duomenis ir tokiu būdu įgalindamas trečiuosius asmenis panaudoti šiuos duomenis pareiškėjo Kortelei prie *Apple Pay* sistemos naujame mobiliajame įrenginyje pridėti, o vėliau ir inicijuoti Operaciją, elgėsi itin aplaidžiai – buvo labai neatsargus.

Kaip jau buvo minėta pirmiau, Mokėjimų įstatymo 34 straipsnyje reglamentuojama viena iš mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigų – naudotis mokėjimo priemone pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas. Kortelės sutarties neatskiriamoje dalyje – Mokėjimo paslaugų teikimo sąlygų 1 priedo 7.1 papunktyje – pareiškėjui, kaip mokėjimo priemonės naudotojui, yra numatytos pareigos: laikytis mokėjimo priemonės išdavimą ir naudojimą reglamentuojančių sąlygų bei imtis veiksmų, kad būtų apsaugoti personalizuoti saugumo duomenys, įskaitant „<...> Naudotojas jokiais atvejais neturi teisės atskleisti tretiesiems asmenims Tapatybės patvirtinimo priemonių ar trečiųjų asmenų pagalba sužinoti Tapatybės patvirtinimo priemones ar kitaip leisti su minėtomis Tapatybės patvirtinimo priemonėmis susipažinti tretiesiems asmenims, įskaitant Banko darbuotojus.“ Be to, Banko mokėjimo paslaugų teikimo sąlygų 7.1 papunktyje, reglamentuojančiame su mokėjimo priemone susijusias banko kliento pareigas, nustatyta, kad „7.1.1. Klientas, turintis teisę naudotis Mokėjimo priemone, privalo: 7.1.1.1. naudotis Mokėjimo priemone pagal Mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, nurodytas atitinkamoje Sutartyje ir/ar Paslaugos sąlygose; 7.1.1.2. sužinojęs apie Mokėjimo

[3] Lietuvos Aukščiausiojo Teismo 2017 m. balandžio 13 d. nutartis civilinėje byloje Nr. e3K-3-180-378/2017, 29 punktas.

priemonės vagystę ar praradimą kitu būdu, įtarus ar sužinojus apie Mokėjimo priemonės neteisėtą įgijimą arba neautorizuotą jos naudojimą, taip pat apie faktus ar įtarimus, kad Mokėjimo priemonės personalizuotus saugumo duomenis (įskaitant Tapatybės patvirtinimo priemones) sužinojo arba jais gali pasinaudoti Tretieji asmenys, nedelsdamas apie tai pranešti Bankui ar kitam jo nurodytam subjektui, vadovaujantis Mokėjimo priemonės išdavimą ir naudojimą reglamentuojančiomis sąlygomis, nurodytomis Sutartyje ir/ar Paslaugos sąlygose. 7.1.2. Klientas, gavęs Mokėjimo priemonę, privalo iš karto imtis visų veiksmų (įskaitant nurodytus Paslaugos sąlygose ir atitinkamoje Sutartyje), kad būtų apsaugoti gautos Mokėjimo priemonės personalizuoti saugumo duomenys (įskaitant Tapatybės patvirtinimo priemones)." Be to, vadovaujantis banko viešai skelbiamomis saugaus naudojimosi elektroninėmis paslaugomis rekomendacijomis, banko klientai raginami nespausti jokių el. paštu, pokalbių programėlėse ar SMS žinutėse gautų nuorodų, nevykdyti prašymų suvesti arba padiktuoti prisijungimo prie interneto banko ar kortelės duomenis, atidžiai įvertinti savo telefono ekrane matomą prašymą įvesti turimos prisijungimo priemonės slaptažodį, jei nėra su kuo sulyginti kontrolinio kodo arba jis nesutampa, arba ignoruoti tokį pranešimą, jei nesiekiama prisijungti prie interneto banko ar inicijuoti mokėjimo operacijų, kilus nors mažiausiai abejonei, neskubėti ir nedelsiant nutraukti veiksmus[4].

Taigi, pirmiau aptartos Kortelės sutarties (ją sudarančių dokumentų) nuostatos aiškiai nustato, kad už mokėjimo ir tapatybės patvirtinimo priemonių personalizuotų saugumo duomenų konfidencialumą yra atsakingas mokėtojas, šiuo atveju – pareiškėjas, kuris privalo užtikrinti, kad minėti duomenys netaptų žinomi tretiesiems asmenims. Atsižvelgiant į tai, manytina, kad pareiškėjo elgesys būtų laikomas kaip atitinkantis mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, jei būtų nustatyta, kad pareiškėjas ėmėsi adekvačių veiksmų (ar priešingai – nustačius, kad nuo tam tikrų veiksmų susilaikė) tam, kad jam banko išduotų mokėjimo priemonių personalizuotų saugumo duomenų, įgalinančių inicijuoti ir tvirtinti mokėjimus, konfidencialumas būtų tinkamai užtikrintas.

Lietuvos bankas, įvertinęs pareiškėjo kreipimesi ir banko atsiliepime nurodytas aplinkybes bei kartu su kreipimusi ir atsiliepimu pateiktus duomenis, nustatė, kad pareiškėjas Operacijos įvykdymo dieną į savo darbo el. paštą gavo tariamą Lietuvos pašto siųstą el. laišką apie gautą siuntą, skirtą pareiškėjui. Šiame pranešime buvo pateikta nuoroda apmokėti 1,90 Eur sumą už tariamai gautą siuntą. Pareiškėjas šalių neginčijamomis aplinkybėmis paspaudė gautame el. laiške pateiktą nuorodą ir pagal ją atsidariusioje interneto svetainėje suvedė tam tikrus savo asmens ir mokėjimo priemonių duomenis, o vėliau per banko mobiliąją programėlę gavo pranešimą apie rezervuotą 250 Eur sumą Operacijai įvykdyti.

Bankas kartu su atsiliepimu Lietuvos bankui pateikė vidinės sistemos duomenis, kurie patvirtina, kad pareiškėjo ginčijama Operacija Kortele buvo inicijuota pasinaudojant *Apple Pay* mokėjimo metodu. Remiantis atsiliepime teikiamais paaiškinimais, tam, kad būtų galima atsiskaityti pasinaudojant *Apple Pay* mokėjimo metodu, visų pirma, būtina mokėjimo kortelę pridėti prie *Apple Pay* sistemos. Mokėjimo kortelei prie *Apple Pay* sistemos pridėti yra taikoma saugesnio autentiškumo patvirtinimo procedūra, kurios metu reikia ne tik pateikti mokėjimo kortelės duomenis, bet ir suvesti vienkartinį saugos kodą, kas, pagal banko pateiktus įrodymus, ir buvo atlikta šiuo atveju. Be to, kaip nurodo bankas atsiliepime, aplinkybę, kad pareiškėjas iš trečiųjų asmenų gavo Lietuvos pašto vardu siųstą suklastotą el. laišką su nurodymais, kuriuos jis įvykdė, t. y. suklastotame interneto puslapyje, atsidariusiame pagal suklastotame Lietuvos pašto pranešime pateiktą nuorodą, suvedė savo mokėjimo priemonių personalizuotus saugumo duomenis, patvirtina ir iš policijos 2022 m. balandžio 27 d. ir 2022 m. balandžio 28 d. banko gauti paklausimai, kuriuose nurodyta: „Ikiteisminio tyrimo metu buvo nustatyta, kad 2022-04-19 nukentėjusysis X. X., gim. (*duomenys neskelbtini*), gavo elektroninį laišką, kuriame buvo nurodyta, kad pašte yra gautas siuntinys ir už pristatymą reikia sumokėti 1.90 eurų, ir paspaudus atsiųstą nuorodą nukentėjusysis buvo nukreiptas į elektroninį puslapį, kur reikėjo suvesti visus mokėjimo kortelės duomenis. Suvedus prašomus duomenis, po kelių dienų X. X. patikrinęs savo sąskaitą pamatė, kad iš sąskaitos buvo atliktas neteisėtas 250 eurų pervedimas į REVOLIUT sąskaitą Dubline."

Lietuvos bankas, siekdamas tinkamai įvertinti Operacijos įvykdymo aplinkybes, kaip prielaidą spręsti ir dėl pareiškėjo neatsargumo laipsnio, ginčo nagrinėjimo metu taip pat paprašė pareiškėjo papildomai paaiškinti, kokius veiksmus, galėjusius lemti Operacijos įvykdymą, pareiškėjas atliko iki jos inicijavimo (taigi, iki pareiškėjo Kortelės pridėjimo prie

[4] https://www.swedbank.lt/static/pdf/legalisation/private/mokejimu_paslaugu_teikimo_salygos_2019-12-09.pdf

Apple Pay sistemos naujame įrenginyje), taip pat ir tai, kokius konkrečiai savo mokėjimo priemonių personalizuotus saugumo duomenis pareiškėjas galėjo atskleisti tretiesiems asmenims. Pateikdamas paaiškinimus, pareiškėjas nurodė, kad Operacijos įvykdymo dieną gavo laišką „apie mano vardu gautą siuntą (apie 14 val). Laiške buvo nuoroda, nukreipianti į post.lt puslapį. Buvo prašoma apmokėti simbolinę sumą (1.90 eur) už siuntą. Suvedžiau mokėjimo kortelės duomenis, adresą ir savo telefono numerį. Po kurio laiko gavau sms su patvirtinimo kodu, jį patvirtinau. Elgiausi drąsiai, nes suma ne didelė. Viskas tuo ir pasibaigė. Po keletos valandų (apie 23 val), sulaukiau pranešimo į telefoną (Per Swedbank programėlę), kad buvo nuo kortelės nuskaičiuota 250 eur suma už pirkinį. Mano jokio įsikišimo tame nebuvo, nebuvo prašoma patvirtinimo per SMART ID ir pan. Suprantu, kad mokėjimo duomenis pateikiau pats, patvirtinimo kodą, kurį gavau SMS žinute įvedžiau pats." Taigi, pareiškėjas iš esmės patvirtina banko poziciją, kad, paspaudęs ant trečiųjų asmenų siųstame pranešime pateiktos nuorodos, pareiškėjas netikrame Lietuvos pašto puslapyje suvedė savo mokėjimo priemonių personalizuotus saugumo duomenis, kurie, kaip paaiškėjo vėliau, įgalino trečiuosius asmenis naujame įrenginyje pridėti Kortelę prie *Apple Pay* sistemos ir inicijuoti bei patvirtinti Operaciją.

Vadinasi, tiek ginčo byloje esančiais duomenimis, tiek ir šalių neginčijamomis aplinkybėmis pareiškėjo Kortelė prie *Apple Pay* sistemos naujame įrenginyje buvo pridėta, suvedus mokėjimo kortelės numerį ir šios kortelės CVC kodą, taip pat būtent į pareiškėjo mobilųjį telefoną siųstą vienkartinį saugos kodą. Todėl, kaip patvirtina pats pareiškėjas, galimai nesuprasdamas atliekamų veiksmų reikšmės bei pasekmių, jis atskleidė tretiesiems asmenims visus duomenis, būtinus jo Kortelei pridėti prie *Apple Pay* sistemos naujame įrenginyje, iš kurio vėliau ir inicijuota Operacija. Pareiškėjui suvedus SMS žinute jo telefono numeriu atsiųstą saugos kodą, Kortelės pridėjimas naujame įrenginyje buvo patvirtintas, o atsiskaitymo *Apple Pay* paslauga aktyvuota – ja naudojantis ir inicijuota bei patvirtinta Operacija. Kaip nurodoma atsiliepime, be pareiškėjo telefono numeriu išsiųsto vienkartinio saugos kodo suvedimo į *Apple Pay* sistemą, pareiškėjo Kortelės pridėjimas nebūtų buvęs patvirtintas ir atsiskaitymas su *Apple Pay* būtų buvęs neįmanomas: įvedus neteisingą saugos kodą, visas procesas yra pradedamas iš naujo, tai yra, vėl prašoma suvesti mokėjimo kortelės duomenis, ši informacija perduodama mokėjimo paslaugų teikėjui, ją patvirtinus yra išsiunčiamas naujas vienkartinis saugos kodas SMS žinute.

Išanalizavęs šias bei visas kitas ginčo nagrinėjimo metu nustatytas aplinkybes ir ginčo byloje esančius duomenis, Lietuvos bankas daro išvadą, kad vis dėlto vertinti pareiškėjo elgesio kaip atsargaus ir apdairaus ar tik neatsargaus šiuo atveju negalima. Kaip matyti iš ginčo nagrinėjimo metu nustatytų aplinkybių, Operaciją tretieji asmenys be pareiškėjo žinios galėjo atlikti tik dėl to, kad pareiškėjas, būdamas labai neatsargus, netinkamai įvykdė Mokėjimų įstatyme (34 straipsnis) ir su banku sudarytoje Kortelės sutartyje įtvirtintus mokėjimo kortelės saugaus naudojimo reikalavimus. Remiantis ginčo byloje esančia pareiškėjui trečiųjų asmenų Lietuvos pašto vardu siųsto pranešimo kopija, matyti, kad jis (t. y. aptariamas pranešimas) galėjo sukurti pirminį įspūdį, kad iš tiesų yra siųstas Lietuvos pašto, nes yra klaidinamai panašus į tikrą, autentišką Lietuvos pašto interneto svetainę. Vis dėlto jei pareiškėjas, prieš spausdamas pranešime pateiktą nuorodą ir atskleisdamas savo mokėjimo priemonių personalizuotus saugumo duomenis, būtų laikęsis bent elementarių atsargumo reikalavimų, jis būtų perskaitęs pranešimo tekstą ir nesudėtingai identifikavęs, kad nors pranešimo tekste vartojami žodžiai su lietuviškais rašmenimis[5], tačiau pati sakinio konstrukcija yra netaisyklinga, jai trūksta loginės prasmės: „Sveiki, Šiandien gavome Jūsų siuntinį ir Jus informuosime kuriuos turite sumokėti norėdami išsiųsti šį paketą jūsų adresu." Pareiškėjas, gavęs trečiųjų asmenų siųstą pranešimą, nedvejodamas (kaip pripažįsta) paspaudė jame pateiktą nuorodą ir suklastotame interneto puslapyje nurodė savo Kortelės personalizuotus saugumo duomenis, o vėliau ir SMS žinute gautą vienkartinį saugos kodą, neįsitikęs nei siųsto pranešimo ir jame pateiktos nuorodos, nei į ją nukreipiančios interneto svetainės autentiškumu bei prašymo atskleisti konfidencialius savo mokėjimo priemonių duomenis tikrumu. Remiantis pareiškėjo paaiškinimais, jis nežinojo tiksliai, kokiu tikslu gavo tariamą Lietuvos pašto pranešimą ir tik darė prielaidą (neturėdamas jokių tokį spėjimą patvirtinančių duomenų), kad šis pranešimas jam siunčiamas dėl naujos kredito kortelės pareiškėjo vardu atsiuntimo, tačiau nepatikrinęs gautos informacijos ir nesuabejojęs jos tikrumu paspaudė ant pranešime pateiktos nuorodos ir suklastotoje interneto svetainėje atskleidė visus prašomus asmens ir mokėjimo priemonių personalizuotus saugumo

[5] Pastaba. Sukčiavimo atakas rengiančių asmenų siunčiamos suklastotos žinutės (pranešimai el. paštu ar kitais kanalais) dažniausiai būna be lietuviškų rašmenų.

duomenis. Be to, kaip nurodo atsiliepime bankas, pareiškėjas neatkreipė dėmesio į tai, kad iš banko SMS žinute gavo *Apple Pay* aktyvavimo kodą, nors pats naudojasi *Android* įrenginiu. Duomenų, kad pareiškėjas būtų anksčiau tokiu būdu gavęs banko siunčiamas korteles ir (arba) tokiu būdu atsiskaitęs už banko ar kitų paslaugos teikėjų paslaugas, ginčo byloje taip pat nėra. Nurodytos aplinkybės leidžia teigti, kad pareiškėjas būtent dėl savo didelio neatsargumo neišsaugojo jo vardu išduotos Kortelės duomenų konfidencialumo – nesiėmė tų saugumo priemonių, kurių privalėjo imtis, kad būtų tinkamai apsaugoti jam suteiktos mokėjimo priemonės duomenys, bei tretiesiems asmenims suteikė vienkartinį saugos kodą, kurį gavo į sau priklausantį telefono numerį trumpąja SMS žinute. Kaip matyti iš pareiškėjo papildomai pateiktų paaiškinimų, pareiškėjas neneigia elgęsis neapdariai ir pripažįsta savo atsakomybę dėl Kortelės pridėjimo prie *Apple Pay* sistemos naujame įrenginyje.

Todėl, konstatavus, kad pareiškėjas, nesilaikydamas jam, kaip mokėtojui, Mokėjimų įstatyme ir sutartyje su banku nustatytų pareigų, susijusių su išduotomis mokėjimo priemonėmis, elgėsi labai neatsargiai, kartu darytina išvada, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, nustatančią, kad tokiu atveju mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai. Dėl šios priežasties, Lietuvos banko vertinimu, bankas neturi pareigos grąžinti (kompensuoti) pareiškėjui neautorizuotos Operacijos lėšų.

Dėl Operacijos patvirtinimo, reikalaujant programėlėje Smart-ID *suvesti PIN kodus*

Pareiškėjui, be kita ko, kelia abejonių banko veiksmų pagrįstumas ir dėl to, kad Operacija buvo įvykdyta, nereikalaujant pareiškėjo Operacijos patvirtinti turima tapatybės patvirtinimo priemone, t. y. suvedant pareiškėjo naudojamos *Smart-ID* paskyros PIN kodus.

Atsižvelgiant į tai, pažymėtina, kad, vadovaujantis pareiškėjo ir banko sutartį sudarančių banko mokėjimo paslaugų teikimo sąlygų 3.3.1 papunkčiu, „<...> Klientas (Mokėtojas) Sutikimą gali pateikti Banko nustatyta arba Banko ir Kliento sutarta forma ir būdu. Raštu pateikiamas Sutikimas turi būti pasirašytas Kliento ar jo teisėto atstovo. Sutikimas taip pat gali būti patvirtinamas Tapatybės patvirtinimo priemonėmis. Atsiskaitant mokėjimo kortele, tam tikrais atvejais Klientas (Mokėtojas) ar jo atstovas Sutikimą taip pat gali patvirtinti pateikdamas mokėjimo kortelės duomenis (pvz.: vardas ir pavardė / pavadinimas, kortelės numeris, galiojimo terminas, CVV2/CVC2 kodas (skaitmenys kitoje mokėjimo kortelės pusėje)), ar Klientui (Mokėtojui) nustatytu eiliškumu atliekant tam tikrus veiksmus (pvz.: mokėjimo kortelės įdėjimas į tam skirtą vietą, konkrečios paslaugos ar prekės užsakymas), kurie jam siūlomi atsiskaitymo vietose, ar pateikdamas Sutikimą kitu būdu, nurodytu konkrečios Mokėjimo paslaugos teikimo sąlygose ar kitoje Sutartyje. Visais šiame punkte numatytais būdais patvirtintas Sutikimas laikomas Kliento (Mokėtojo) tinkamai patvirtintu, turintis tokią pačią teisinę galią kaip ir tokio Kliento (jo atstovo) pasirašytas popierinis dokumentas (Sutikimas), yra leistinas kaip įrodinėjimo priemonės sprendžiant Banko ir Kliento ginčus teismuose bei kitose institucijose.“

Banko mokėjimo paslaugų teikimo sąlygų 1 priedo „Bekontakčių atsiskaitymų išmaniuoju įrenginiu paslauga“ nuostatose nurodyta, kad „bekontakčių atsiskaitymų išmaniuoju įrenginiu paslauga teikiama per „Swedbank“ ar mokėjimo kortelės turėtojo pasirinkto Banko leidžiamo kito paslaugų teikėjo išmaniąją programėlę (toliau – Išmanioji programėlė). Mokėjimo kortelės turėtojas, pradėdamas naudotis bekontakčių atsiskaitymų išmaniuoju įrenginiu paslauga, per Išmaniąją programėlę susieja išmanųjį įrenginį (pvz., išmanųjį telefoną, išmanųjį laikrodį ir pan.), kuriame yra įdiegta Išmanioji programėlė, su mokėjimo kortele, tokiu būdu sukuriant skaitmeninę mokėjimo kortelės versiją, kuri yra unikali konkretaus išmanaus įrenginio ir mokėjimo kortelės duomenų kombinacija.“ (1 punktas). Be to, pagal minėtų „Bekontakčių atsiskaitymų išmaniuoju įrenginiu paslauga“ nuostatų 2 punktą, „skaitmeninė kortelė, saugoma išmaniajame įrenginyje, mokėjimo kortelės turėtojo bus naudojama atliekant bekontakčių atsiskaitymų išmaniuoju įrenginiu Mokėjimo operacijas. *Esant aktyviai bekontakčių atsiskaitymų išmaniuoju įrenginiu paslaugai mokėjimo kortelės turėtojas galės pateikti Bankui leidžiamus Mokėjimo nurodymus naudodamasis skaitmenine kortele, priklausomai nuo Išmaniosios programėlės paslaugos teikėjo nustatytų reikalavimų autorizuojant Mokėjimo operacijas tokio paslaugos teikėjo nurodytu būdu*.“ Bankas atsiliepime paaiškino, kad Kortelės sutarties sudarymo metu bei bet kuriuo metu vėliau banko interneto banko aplinkoje pareiškėjas turėjo galimybę pasirinkti – įjungti ar išjungti bekontaktį atsiskaitymą Kortele. Bekontakčio atsiskaitymo galimybė Kortelei buvo įjungta 2021 m. gegužės 12 d. 17:57:10 val. ir išjungta nebuvo iki pat Kortelės blokavimo.

Būtina pažymėti, kad šiuo atveju Kortelės pridėjimas naujame įrenginyje prie jame įdiegto *Apple Pay* atsiskaitymo būdo buvo atliktas taikant saugesnę autentiškumo patvirtinimo procedūrą, t. y. panaudojant pareiškėjo iš banko asmeniškai gautą *Apple Pay* vienkartinį saugos kodą, kurį, kaip nustatyta ginčo nagrinėjimo metu, tretiesiems asmenims dėl didelio neatsargumo atskleidė pats pareiškėjas. Kaip paaiškino bankas atsiliepime ir kaip matyti iš pirmiau cituotų Banko mokėjimo paslaugų teikimo sąlygų 1 priedo „Bekontakčių atsiskaitymų išmaniuoju įrenginiu paslauga" nuostatų, autentifikavimo procedūra Operacijos patvirtinimo metu buvo atliekama trečiųjų asmenų valdomame įrenginyje, prie kurio buvo pridėta pareiškėjo Kortelė, *Apple Pay* taikomomis sąlygomis. Taigi, pati Operacija pareiškėjo vardu buvo patvirtinta, taikant saugesnio autentiškumo patvirtinimo procedūrą, kaip nustatyta Mokėjimų įstatymo 58 straipsnio 1 dalyje[6], tačiau naudojantis jau arba tame įrenginyje įdiegtos el. piniginės *Apple Wallet* slaptažodžiu, arba biometriniais duomenimis (piršto atspaudu), arba veido atpažinimo technologiją (angl. *Face ID*), t. y. tokiu būdu, kuris yra numatytas *Apple Pay* naudojimosi sąlygose, su kuriomis sutiko tretieji asmenys Kortelės pridėjimo prie *Apple Pay* metu[7].

Dėl mokėjimo nurodymo neatšaukiamumo

Pareiškėjas kreipimesi, be kita ko, pažymi, kad nurodė, jog kreipėsi į banką, kai Operacijos lėšos iš jo Sąskaitos dar nebuvo nurašytos, todėl bankas turėjo galimybę sustabdyti Operacijos vykdymą.

Vertinant galimybę atšaukti pareiškėjo vardu pateiktą mokėjimo nurodymą įvykdyti Operaciją, papildomai pažymėtina, kad, pagal Mokėjimų įstatymo 44 straipsnio 1 dalį, mokėjimo paslaugų vartotojas negali atšaukti mokėjimo nurodymo po to, kai jį gauna mokėtojo mokėjimo paslaugų teikėjas, išskyrus šiame straipsnyje nustatytas išimtis. Minėto Mokėjimų įstatymo straipsnio 4 dalyje taip pat nustatyta, kad, pasibaigus 1 dalyje nurodytam laikotarpiui, mokėjimo nurodymas gali būti atšauktas tik tuo atveju, kai dėl to susitaria mokėjimo paslaugų vartotojas ir atitinkamas mokėjimo paslaugų teikėjas, o šio straipsnio 2 dalyje numatytais atvejais būtinas ir gavėjo sutikimas. Mokėjimo paslaugų teikėjas gali imti komisinį atlyginimą už mokėjimo nurodymo atšaukimą, jeigu tai numatyta bendrojoje sutartyje. Taigi, pasibaigus Mokėjimų įstatymo 44 straipsnio 1 dalyje nurodytam terminui, mokėjimo nurodymas gali būti atšauktas tik dėl to susitarus vartotojui ir jo mokėjimo paslaugų teikėjui, todėl nurodytos galimybės (t. y. mokėjimo nurodymo atšaukimo) įtvirtinimas Mokėjimų įstatyme neturėtų būti vertinamas kaip priverstinis lėšų grąžinimas mokėtojui, esant jo atitinkamam prašymui (pasibaigus 44 straipsnio 1 dalyje nurodytam terminui).

Mokėjimo paslaugų teikimo sąlygų, kurios yra neatskiriama Kortelės sutarties dalis, 3.3.5.2 papunktyje nustatyta: „kai Mokėjimo operacija inicijuojama Gavėjo ar per Gavėją (pvz.: atsiskaitymas mokėjimo kortele), ar inicijuojama Mokėjimo inicijavimo paslaugos teikėjo, Mokėtojas negali atšaukti Mokėjimo nurodymo po to, kai Mokėjimo inicijavimo paslaugos teikėjui pateikė Sutikimą inicijuoti Mokėjimo operaciją arba Mokėtojas Gavėjui davė Sutikimą atlikti Mokėjimo operaciją. <…>".

Bankas atsiliepime paaiškino, kad mokėjimo operacijų mokėjimo kortelėmis vykdymas skiriasi nuo įprastų kredito pervedimų, nes lėšos iš su mokėjimo kortele susietos sąskaitos operacijų mokėjimo kortelėmis atveju nėra nurašomos ir pervedamos tiesiogiai gavėjo mokėjimo paslaugų teikėjui, o tik rezervuojamos sąskaitoje tuo tikslu, kad nebūtų naudojamos kitoms mokėtojo inicijuojamoms operacijoms Sąskaitoje vykdyti (Kortelės sutarties 4.6 papunktis). Bankas paaiškino, kad gavėjo mokėjimo paslaugų teikėjas tokios operacijos lėšas nusirašo tiesiogiai iš banko korespondentinės sąskaitos, o iš mokėtojo sąskaitos lėšas bankas nurašo tik tuomet, kai gauna mokėjimo operacijų finansinius patvirtinimus – pranešimus, kad lėšos nurašytos iš banko korespondentinės sąskaitos.

Ginčo nagrinėjimo metu nustatytais duomenimis, šiuo atveju nei Mokėjimų įstatyme, nei šalių susitarime nurodytos sąlygos atšaukti mokėjimo nurodymą įvykdyti Operaciją nagrinėjamo ginčo atveju nebuvo nustatytos, t. y. pareiškėjas į banką su prašymu atšaukti mokėjimo nurodymą įvykdyti Operaciją ir (arba) grąžinti šio mokėjimo lėšas į pareiškėjo

---

[6] Mokėjimų įstatymo 58 straipsnio 1 dalyje nustatyta: „Mokėjimo paslaugų teikėjas privalo taikyti saugesnio autentiškumo patvirtinimo procedūrą, kai mokėtojas: 1) internetu arba kitomis nuotolinio ryšio priemonėmis prisijungia prie savo mokėjimo sąskaitos; 2) inicijuoja elektroninę mokėjimo operaciją; 3) nuotolinio ryšio priemone vykdo bet kokį veiksmą, kuris gali būti susijęs su sukčiavimo atliekant mokėjimą ar kitokio piktnaudžiavimo rizika."

[7] Daugiau informacijos apie naudojimąsi *Apple Pay* paslauga (atsiskaitymo metodu) bankas pateikia savo interneto svetainėje https://www.swedbank.lt/private/cards/paymentSolutions/applepay?language=LIT.

Sąskaitą paskambino po to, kai Operacija jau buvo įvykdyta, taigi ir Mokėjimų įstatyme bei šalių susitarime nustatytas terminas atšaukti mokėjimo nurodymus jau buvo praėjęs, ir bankas neturėjo jokių galimybių Operaciją atšaukti.

Bankas pažymi, kad net ir tuo atveju, jei Operacijos rezervacija būtų buvusi panaikinta Sąskaitoje, tačiau gavėjo mokėjimo paslaugų teikėjui Operacijų sumą nusirašius iš banko korespondentinės sąskaitos, bankas teisėtai ir pagrįstai būtų turėjęs teisę susigrąžinti dėl pareiškėjo kaltės, pasireiškusios dideliu neatsargumu, įvykdytos Operacijos sumą iš pareiškėjo Sąskaitos (Kortelės sutarties 4.6 ir 6.3 papunkčiai).

Pareiškėjui taip pat kelia abejonių banko veiksmų pagrįstumas dėl to, kad nors Kortelės funkcionalumas buvo apribotas, tačiau, nepaisant šios aplinkybės, Operacija vis tiek buvo įvykdyta. Būtina pažymėti, kad, pagal Mokėjimų įstatymo 46 straipsnį, mokėjimo paslaugų teikėjas privalo užtikrinti, jog po mokėjimo nurodymo gavimo mokėjimo operacijos suma būtų įskaityta į mokėjimo nurodyme nurodyto gavėjo sąskaitą minėtame straipsnyje nustatytais terminais, o Mokėjimų įstatymo 51 straipsnio 1 dalyje nustatyta mokėjimo paslaugų teikėjo atsakomybė už mokėtojo inicijuotos mokėjimo operacijos neįvykdymą, netinkamą ar pavėluotą įvykdymą. Aplinkybė, kad pareiškėjo ginčijama Operacija iš tiesų yra neautorizuota, nors ir atitiko pareiškėjo ir banko sutartą sutikimo mokėjimo operacijai davimo tvarką, paaiškėjo vėliau, nei ši Operacija buvo inicijuota, patvirtinta ir įvykdyta, ir bankas neturėjo teisės aktuose nustatyto pagrindo tokio mokėjimo nurodymo (t. y. mokėjimo nurodymo įvykdyti Operaciją) nevykdyti. Ginčo nagrinėjimo metu nustatytais duomenimis, Operacija buvo įvykdyta dar iki Kortelės funkcionalumas buvo apribotas bei ji buvo blokuota[8].

Dėl lėšų grąžinimo procedūros inicijavimo pagal tarptautinės mokėjimo kortelių organizacijos Mastercard *taisykles*

Papildomos galimybės mokėjimo kortelės turėtojui susigrąžinti mokėjimo kortele įvykdytų mokėjimo operacijų lėšas nustatytos tarptautinės mokėjimo kortelių organizacijos *Mastercard* taisyklėse. Vadovaudamasis šiose taisyklėse nustatytais atvejais ir tvarka, bankas, gavęs kliento prašymą, gali kreiptis į tarptautinę mokėjimo kortelių organizaciją *Mastercard* dėl lėšų grąžinimo procedūros taikymo[9]. Taigi banko veiksmai, ginčijant mokėjimo operacijas, atliktas mokėjimo kortele, reglamentuoti pirmiau minėtose *Mastercard* taisyklėse, ir nei Lietuvos Respublikos teisės aktai, nei Europos Sąjungos teisės aktai nereglamentuoja, kokiomis sąlygomis turi būti vykdomos tokios lėšų grąžinimo procedūros.

Bankas, pagrįsdamas atsisakymą pareiškėjo prašymu inicijuoti lėšų grąžinimo procedūrą dėl Operacijos tarptautinės mokėjimo kortelių organizacijos *Mastercard* nustatyta tvarka, nurodo, kad, pagal tarptautinės mokėjimo kortelių organizacijos *Mastercard* taisykles, bankas, kaip kortelę išdavęs mokėjimo paslaugų teikėjas, neturi teisės inicijuoti ginčo taisyklėse numatyta tvarka, jei kortelės naudotojas operaciją ginčija kaip ne jo autorizuotą, o operacija patenka į taisyklėse išvardytų sąrašą[10]. Bankas pažymi, kad ginčijama Operacija patenka į minėtose taisyklėse išvardytą sąrašą kaip *Properly authenticated and identified transactions*, nes Operacijai įvykdyti buvo naudojamas *Mastercard* taisyklėse nurodytas *Identity Check and Digital Secure Remote Payment* (DSRP) procesas. Taigi, tarptautinės mokėjimo kortelių organizacijos *Mastercard* taisyklės, kaip nurodo bankas, nenustato galimybės ginčyti mokėjimo kortele įvykdytų operacijų kaip ne mokėtojo autorizuotų, jei jų autorizavimo procese buvo taikomas sustiprintas mokėtojo tapatybės nustatymo procesas. Toks procesas taikomas atsiskaitymams mokėjimo kortele naudojant žymenis (angl. *tokenisation*), t. y. tokiu būdu, kaip buvo įvykdyta Operacija.

Lietuvos banko vertinimu, ginčo byloje nėra duomenų, kurie leistų teigti, kad, bankui bandžius inicijuoti lėšų grąžinimo procedūrą dėl pareiškėjo ginčijamos Operacijos, tokia procedūra būtų buvusi sėkminga. Kitaip tariant, bankas atsiliepime pateikė motyvus – nurodė tarptautinės mokėjimo kortelių organizacijos *Mastercard* taisyklių nuostatas, pagal kurias ginčo procedūra minėtų taisyklių nustatyta tvarka dėl pareiškėjo ginčijamos Operacijos nėra galima.

Todėl, įvertinus visa tai, kas išdėstyta pirmiau, ir nustačius, jog yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, darytina išvada, kad pareiškėjo banko atžvilgiu

[8] Operacija įvykdyta 2022 m. balandžio 19 d. 23:33:42 val. Lietuvos laiku, o Kortelės funkcionalumas apribotas 2022 m. balandžio 19 d. 23:37:04 val.

[9] Teisės aktai nereglamentuoja, kokiomis sąlygomis turi būti vykdomos tokios lėšų grąžinimo procedūros, nes tai nustato konkreti mokėjimo kortelių organizacija savo parengtose lėšų grąžinimo (angl. *chargeback*) taisyklėse.

[10] Tarptautinės mokėjimo kortelių organizacijos *Mastercard* taisyklių sąlyga originalo, t. y. anglų, kalba: „A No Cardholder Authorization chargeback must not be processed for any of the following."

keliamas reikalavimas grąžinti Operacijos sumą – 250 Eur yra nepagrįstas, todėl atmestinas.

Remdamasis tuo, kas išdėstyta, ir vadovaudamasis Lietuvos Respublikos vartotojų teisių apsaugos įstatymo 27 straipsnio 1 dalies 3 punktu, Lietuvos banko valdybos 2012 m. sausio 26 d. nutarimo Nr. 03-23 „Dėl Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių patvirtinimo" 2 punktu ir šiuo nutarimu patvirtintų Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių 59.3 papunkčiu, n u s p r e n d ž i u:

Atmesti pareiškėjo X. X. reikalavimą.

Lietuvos banko sprendimas dėl ginčo esmės yra rekomendacinio pobūdžio ir teismui neskundžiamas. Vartotojui ir finansų rinkos dalyviui išlieka teisė dėl ginčo sprendimo kreiptis į teismą arba kitą ginčų nagrinėjimo instituciją įstatymų nustatyta tvarka. Kreipimasis į teismą po Lietuvos banko sprendimo dėl ginčo esmės priėmimo nelaikomas šio sprendimo apskundimu. Ginčo šalys turi pareigą pranešti Lietuvos bankui, jeigu viena iš ginčo šalių pareiškia ieškinį bendrosios kompetencijos teismui prašydama nagrinėti tapatų ginčą iš esmės.

Direktorius Arūnas Raišutis