



**LIETUVOS BANKO
TEISĖS IR LICENCIJAVIMO DEPARTAMENTO
DIREKTORIUS**

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

2022 m. liepos 20 d. Nr. 429-320
Vilnius

Lietuvos bankas gavo X. X. (toliau – pareiškėja) kreipimąsi, kuriuo prašoma išnagrinėti tarp pareiškėjos ir „Swedbank“, AB, (toliau – bankas) kilusį ginčą.

N u s t a t y t a:

2022 m. balandžio 16 d. ir 2022 m. balandžio 17 d. banko pareiškėjai išduota *Mastercard* mokėjimo kortele Nr. (*duomenys neskelbtini*) (toliau – Kortelė), panaudojant *Apple Pay* mokėjimo metodą, įvykdytos dvi mokėjimo operacijos: mokėjimo operacija, kurios suma 265 Eur, gavėjui *Le Matignon*, ir atitinkamai mokėjimo operacija, kurios suma 263,20 Eur, gavėjui *Vinted* (toliau – Operacijos).

2022 m. balandžio 17 d. 16:19 val. pareiškėja kreipėsi telefonu į banką, ginčydama Operacijų įvykdymą. Pokalbio su banko darbuotoja metu 16:30:13 val. pareiškėjos Kortelė buvo blokuota, pareiškėjai informavus, kad jos su Kortele susietoje banko sąskaitoje buvo įvykdytos pareiškėjos neautorizuotos Operacijos. Pokalbio metu pareiškėja nurodė, kad gavo pranešimą apie iš elektroninės parduotuvės *Aliexpress* pareiškėjos vardu gautą siuntą. Minėtame pranešime pareiškėjos buvo prašoma sumokėti 2 Eur mokestį už minėtos siuntos per *LP Express* siuntų tarnybą atsiuntimą. Pokalbio metu pareiškėja patvirtino, kad suvedė Kortelės duomenis, taip pat aplinkybę, kad gavo SMS pranešimą iš banko su vienkartinio saugos kodu.

2022 m. balandžio 19 d. prekybininkas *Vinted* grąžino vienos iš Operacijų (t. y. 263,20 Eur) sumą į pareiškėjos su Kortele susietą sąskaitą banke.

Pareiškėja ginčija banko sprendimą negražinti ir (arba) nekompensuoti jai gavėjui *Le Matignon* atliktos mokėjimo Operacijos sumos – 265 Eur. Kreipimesi pareiškėja nurodo, kad 2022 m. balandžio 17 d. gavo žinutę, kad jos Kortelės sąskaitoje yra rezervuotos Operacijų sumos gavėjams *Vinted* ir *Le Matignon*. Žinodama, kad jokių prekių ji neužsakė, pareiškėja nurodo iškart susisiekti su budinčiu banko darbuotoju ir informavusi apie Operacijas, kurių ji pati neatliko. Pareiškėjos teigimu, banko darbuotoja užblokavo jos Kortelę ir nurodė, kad jokie mokėjimai nebus įvykdyti. Pareiškėja taip pat nurodo, kad 2022 m. balandžio 19 d. sulaukė vienos iš Operacijų gavėjui *Vinted* sumos grąžinimo, tačiau 2022 m. balandžio 21 d. banko buvo informuota, kad kitos Operacijos suma – 265 Eur, pervesta gavėjui *Le Matignon*, pareiškėjai nebus grąžinta ar kitaip kompensuota. Su tokia banko pozicija pareiškėja nesutinka. Pareiškėja teigia, kad laiku informavo banką apie neautorizuotas Operacijas, t. y. dar tada, kai lėšos jos Kortelės sąskaitoje buvo tik rezervuotos, todėl mano, kad bankas jai turi grąžinti ir antros Operacijos, atliktos gavėjo *Le Matignon* naudai, sumą – 265 Eur.

Bankas nesutinka tenkinti pareiškėjos reikalavimo. Atsiliepime nurodoma, kad, banko duomenimis, pareiškėjos nuostoliai (265 Eur) dėl Operacijos atsirado dėl to, kad Kortelė buvo pridėta elektroninėje pinigineje *Apple Wallet*, įdiegtoje *Apple* išmaniajame įrenginyje (išmaniajame telefone, planšetiniame kompiuteryje, išmaniajame laikrodyje ir pan.), kuriuo tretieji asmenys galėjo panaudoti *Apple Pay* išmanųjį atsiskaitymo būdą ir tokiu būdu Kortele inicijuoti Operacijas nenaudodami Kliento faktiškai turimos plastikinės Kortelės. Bankas pažymi, kad pareiškėjos, kaip Kortelės naudotojos, tapatybė buvo nustatyta taikant sustiprintą mokėtojo tapatybės nustatymo būdą (pareiškėjai asmeniškai atsiųstas vienkartinis kodas) Kortelės pridėjimo prie kitame įrenginyje aktyvuojamo *Apple Pay* mokėjimo metodo metu, t. y. buvo laikomasi saugesnio autentiškumo patvirtinimo reikalavimų naudojant technologijas, kuriomis galima užtikrinti saugų vartotojo autentiškumo patvirtinimą. Bankas teigia, kad galimybė tretiesiems asmenims pridėti pareiškėjos Kortelę jų valdomame įrenginyje prie *Apple*

Pay sistemos atsirado tik dėl to, kad pareiškėja perdavė tretiesiems asmenims Kortelės duomenis bei iš banko SMS žinute gautą Kortelės pridėjimo prie *Apple Pay* sistemos vienkartinį saugos kodą – tokiu būdu pareiškėjos vardu buvo duoti sutikimai Kortelei su ja susietoje banko sąskaitoje įvykdyti Operacijas. Minėtą Kortelės pridėjimo prie *Apple Pay* sistemos vienkartinį saugos kodą bankas nurodo išsiuntęs pareiškėjos telefono numeriu 2022 m. balandžio 16 d. 09:44:25 val., SMS žinutėje nurodydamas: „Jūsų kortelės pridėjimo prie *Apple Pay* patvirtinimo kodas yra (*duomenys neskelbtini*). Šis kodas galios 30 minučių.“ Bankas mano, kad gavusi šią žinutę pareiškėja, pagal žinutės turinį matydama veiksmus, kurių ji neatlieka, turėjo susilaikyti nuo tolesnių veiksmų, jeigu neketino Kortelės pridėti prie *Apple Pay* sistemos, tačiau Operacijos buvo inicijuotos tretiesiems asmenims ne tik sužinojus ir panaudojus pareiškėjos Kortelės personalizuotus saugumo duomenis, bet ir pirmiau minėtą SMS žinute gautą vienkartinį saugos (kortelės pridėjimo prie *Apple Pay* sistemos) kodą. Bankas teigia, kad tokiu būdu pareiškėja pažeidė jai, kaip mokėtojai, Kortelės sutartyje su banku ir teisės aktuose nustatytas pareigas, todėl visi dėl Operacijų iki Kortelės blokavimo kilę nuostoliai turi tekti pareiškėjai. Bankas mano, kad nuostolius dėl Operacijos pareiškėja patyrė dėl savo didelio neatsargumo: gavusi iš banko SMS žinutę su pridėjimo prie *Apple Pay* sistemos kodu, pareiškėja galėjo suprasti, kad šis kodas nėra skirtas sumokėti už siuntų tarnybos paslaugas, todėl turėjo susilaikyti nuo tolesnių veiksmų, tačiau to nepadarė, taip pažeisdama jai, kaip mokėtojai, su mokėjimo priemonių naudojimu nustatytas pareigas. Bankas prašo atmesti pareiškėjos 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.

Pareiškėjos ir banko ginčas kilo dėl banko atsisakymo gražinti pareiškėjai jos Kortelei, panaudojant *Apple Pay* mokėjimo metodą, vienos iš atliktų Operacijų¹, kurios vertė – 265 Eur ir kurios atlikti pareiškėja teigia nedavusi sutikimo, sumą.

Pareiškėja neigia autorizavusi Operaciją ir (arba) pridėjusi savo Korteles prie *Apple Pay* sistemos naujame įrenginyje bei tvirtina, kad lėšos iš jos Kortelės sąskaitos buvo nurašytos dėl to, kad tretieji asmenys galėjo pasisavinti pareiškėjos Kortelės duomenis. Pareiškėja taip pat pažymi, kad ji į banką ginčydamą Operacijas kreipėsi dar tada, kai Operacijų lėšos pareiškėjos Kortelės sąskaitoje buvo dar tik rezervuotos, todėl bankas turi gražinti ir (arba) kompensuoti pareiškėjai negražintos Operacijos sumą. Atsiliepime bankas nurodo, kad Operacija Kortelei įvyko ne dėl sutrikimų banko ar tarptautinės mokėjimo kortelių organizacijos *Mastercard* sistemoje arba saugumo spragų jose, o dėl pareiškėjos veiksmų, kuriais tretiesiems asmenims buvo atskleisti pareiškėjos mokėjimo priemonių personalizuoti saugumo duomenys, dėl to tretieji asmenys įgijo galimybę savo įrenginiu inicijuoti Operacijas pareiškėjos Kortelės 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 pareiškėjos ginčijama Operacija buvo atlikta naudojantis trečiųjų asmenų įrenginyje įdiegtu *Apple Pay* mokėjimo būdu, prie atitinkamo įrenginio, kuriame veikia *Apple Pay* sistema, pridėjus pareiškėjos Korteles. Taigi, šalių neginčijamomis aplinkybėmis, Operacija buvo inicijuota ir įvykdyta trečiųjų asmenų, jiems neteisėtu būdu sužinojus (pasisavinus) pareiškėjos mokėjimo priemonių personalizuotus saugumo duomenis ir juos panaudojus naujame įrenginyje pridėti pareiškėjos Korteles prie *Apple Pay* sistemos, kuria

¹ Operacija, įvykdyta gavėjui *Le Matignon*.

pasinaudojant vėliau inicijuota ir įvykdyta pati Operacija. Akivaizdu, kad Operacijos inicijavimas ir patvirtinimas neatitiko pačios pareiškėjos valios, nors formaliai (išoriniais požymiais) ir sutapo su pareiškėjos ir banko sutarta sutikimo mokėjimo operacijoms davimo forma ir tvarka. Pareiškėjos nurodytos aplinkybės, kad Operacija nėra pareiškėjos autorizuota, o pareiškėjos Kortelę prie *Apple Pay* sistemos naujame įrenginyje pridėjo ne pareiškėja, o tretieji asmenys, bankas atsiliepime neginčija, todėl šio ginčo nagrinėjimo metu Lietuvos bankas daro išvadą, kad Operacija, atlikta nesant pareiškėjos valios ir jai net nežinant apie Operacijos inicijavimo aplinkybę bei neišreiškus jokių valinių veiksmų Operacijai patvirtinti, laikytina neautorizuota.

Dėl neautorizuotų mokėjimo operacijų pasekmių ir pareiškėjos teisės į Operacijos sumos gražinimą

Pagal Mokėjimų įstatymo 38 straipsnio 1 dalį, mokėtojo mokėjimo paslaugų teikėjas privalo gražinti 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 nustatyta, 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 didžiausias 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 įstatyme aiškiai nustatyta, 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 gražinti 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 pareiškėja galėjo veikti nesąžiningai arba tyčia, įskaitant sukčiavimą, nėra. Tai reiškia, kad, siekiant įvertinti, ar bankas pagrįstai atsisako kompensuoti pareiškėjos nuostolius, susijusius su Operacijos įvykdymu, ir ar galėtų pareiškėjos atžvilgiu būti taikoma Mokėjimų įstatymo 39 straipsnio 3 dalis, būtina nustatyti, ar pareiškėjos elgesys, atskleidžiant tam tikrus personalizuotus mokėjimo priemonės (banko išduotos Kortelės) požymius, ir (arba) kiti veiksmai, dėl kurių galėjo būti įvykdyta Operacija, vertintini kaip didelis pareiškėjos neatsargumas, dėl kurio visi jos reikalaujami atlyginti nuostoliai turėtų tekti pačiai pareiškėjai.

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“².

Bankas mano, kad nuostolius dėl Operacijos pareiškėja patyrė dėl savo didelio neatsargumo, t. y. pareiškėja, perduodama tretiesiems asmenims savo Kortelės duomenis (Kortelėje nurodytus savo vardą, pavardę, kortelės numerį ir CCV kodą) bei vienkartinį banko pareiškėjai jos 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 Kortelės sąskaitoje vykdyti mokėjimo operacijas Kortele pareiškėjos 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 pareiškėjos nuostolių dėl neautorizuotos Operacijos įvykdymo galėtų būti vertinamas kaip pagrįstas tik tuo atveju, jei būtų įrodyta, kad pareiškėja, atskleisdama tam tikrus personalizuotus savo mokėjimo priemonių saugumo duomenis ir tokiu būdu įgalindama trečiuosius asmenis panaudoti šiuos duomenis pareiškėjos Kortelei prie *Apple Pay* sistemos naujame mobilajame įrenginyje pridėti, o vėliau ir inicijuoti Operaciją (Operacijas), elgėsi itin aplaidžiai – buvo labai neatsargi.

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 pareiškėjai, kaip mokėjimo priemonės naudotojai, 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 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 nespaušti 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

² Lietuvos Aukščiausiojo Teismo 2017 m. balandžio 13 d. nutartis civilinėje byloje Nr. e3K-3-180-378/2017, 29 punktas.

matomą prašymą įvesti turimos prisijungimo priemonės slaptažodį, jei nėra su kuo sulygtinti kontrolinio kodo arba jis nesutampa, arba ignoruoti tokį pranešimą, jei nesiekiami prisijungti prie interneto banko ar inicijuoti mokėjimo operacijų, kilus nors mažiausiai abejonei, neskubėti ir nedelsiant nutraukti veiksmus³.

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 – pareiškėja, kuri privalo užtikrinti, kad minėti duomenys netaptų žinomi tretiesiems asmenims. Atsižvelgiant į tai, manytina, kad pareiškėjos elgesys būtų laikomas kaip atitinkantis mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, jei būtų nustatyta, kad pareiškėja ėmėsi adekvačių veiksmų (ar priešingai – nustačius, kad nuo tam tikrų veiksmų susilaikė) tam, kad jai banko išduotų mokėjimo priemonių personalizuotų saugumo duomenų, įgalinančių inicijuoti ir tvirtinti mokėjimus, konfidencialumas būtų tinkamai užtikrintas.

Lietuvos bankas, įvertinęs pareiškėjos kreipimesi ir banko atsiliepime nurodytas aplinkybes bei kartu su kreipimusi ir atsiliepimu pateiktus duomenis, nustatė, kad pareiškėja prieš Operacijų įvykdymą gavo tariamą Lietuvos pašto vardu siųstą pranešimą apie gautą siuntą, skirtą pareiškėjai. Šiame pranešime, pareiškėjos teigimu, buvo pateikta nuoroda apmokėti 2 Eur sumą už tariamai gautą siuntą iš elektroninės parduotuvės *Aliexpress*. Pareiškėja, šalių neginčijamomis aplinkybėmis, paspaudė gautame pranešime 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 rezervuotas 265 Eur ir 263,20 Eur sumas Operacijoms įvykdyti.

Bankas kartu su atsiliepimu Lietuvos bankui pateikė vidinės sistemos duomenis, kurie patvirtina, kad abi pareiškėjos ginčijamos Operacijos Kortele buvo inicijuotos 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. Aplinkybę, kad, paspaudusi gautame pranešime pateiktą nuorodą, galimai suklastotoje Lietuvos pašto interneto svetainėje visus savo mokėjimo kortelės duomenis suvedė, taip pat kad panaudojo iš banko SMS žinute gautą vienkartinį kodą, pripažįsta ir pati pareiškėja, kaip matyti iš banko kartu su atsiliepimu pateiktos pareiškėjos ir banko darbuotojos pokalbio, vykusio 2022 m. balandžio 17 d., stenogramos.

Vadinasi, ginčo byloje esančiais duomenimis, tiek ir šalių neginčijamomis aplinkybėmis, pareiškėjos Kortelė prie *Apple Pay* sistemos naujame įrenginyje buvo pridėta, suvedus pačios pareiškėjos pateiktus personalizuotus saugumo duomenis, taip pat būtent į pareiškėjos mobilųjį telefoną siųstą vienkartinį saugos kodą. Todėl, kaip patvirtina pati pareiškėja, galimai nesuprasdama atliekamų veiksmų reikšmės bei pasekmių, ji atskleidė tretiesiems asmenims visus duomenis, būtinus jos Kortelei pridėti prie *Apple Pay* sistemos naujame įrenginyje, iš kurio vėliau ir inicijuotos abi pareiškėjos neautorizuotos Operacijos. Pareiškėjai suvedus SMS žinute jos telefono numeriu atsiųstą saugos kodą, Kortelės pridėjimas naujame įrenginyje buvo patvirtintas, o atsiskaitymo *Apple Pay* paslauga aktyvuota – ja naudojantis ir inicijuota bei patvirtinta ir Operacija gavėjui *Le Matignon*, kurios suma pareiškėjai nėra iki šiol gražinta. Kaip nurodoma atsiliepime, be pareiškėjos telefono numeriu išsiųsto vienkartinio saugos kodo suvedimo į *Apple Pay* sistemą, pareiškėjos Kortelės pridėjimas nebūtų buvęs patvirtintas ir atsiskaitymas su *Apple Pay* būtų buvęs neįmanomas: įvedus neteisingą saugos kodą, visas procesas pradedamas iš naujo, t. y. vėl prašoma suvesti mokėjimo kortelės duomenis, ši informacija perduodama mokėjimo paslaugų teikėjui, ją patvirtinus 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 pareiškėjos elgesio kaip atsargaus ir apdairaus ar tik neatsargaus šiuo atveju negalima. Kaip matyti iš ginčo nagrinėjimo metu nustatytų aplinkybių, Operaciją tretieji asmenys be pareiškėjos žinios galėjo atlikti tik dėl to, kad pareiškėja, būdama labai neatsargi, netinkamai įvykdė Mokėjimų įstatyme (34 straipsnis) ir su banku sudarytoje Kortelės sutartyje įtvirtintus mokėjimo kortelės saugaus naudojimo reikalavimus. Remiantis ginčo nagrinėjimo metu nustatytais duomenimis, pareiškėja

³ https://www.swedbank.lt/static/pdf/legalisation/private/mokejimu_paslaugu_teikimo_salygos_2019-12-09.pdf

nebuvo užsisakiusi prekių ir nelaukė siuntinio pristatymo (pranešimo apie siuntinio pristatymą), tačiau gavusi trečiųjų asmenų siųstą pranešimą apie tariamai gautą siuntinį iš elektroninės parduotuvės *Aliexpress*, iš kurios pareiškėja teigia prekių neįsigijusi, jo patikimumu nesudvejojo ir įvykdė pranešime pateiktus nurodymus. Taigi, pareiškėja, gavusi trečiųjų asmenų siųstą pranešimą, nedvejodama (kaip pripažįsta) paspaudė jame pateiktą nuorodą ir suklastotoje interneto svetainėje nurodė savo Kortelės personalizuotus saugumo duomenis, o vėliau ir SMS žinute iš banko gautą vienkartinį saugos kodą, neįsitikinusi nei siųsto pranešimo ir jame pateiktos nuorodos, nei į ją nukreipiančios interneto svetainės autentiškumu bei prašymo atskleisti konfidencialius savo mokėjimo priemonių duomenis tikrumu. Tad nors kreipimesi Lietuvos bankui pareiškėja teigia, kad, gavusi banko pranešimus apie įvykdytas Operacijas, ji suprato, jog galėjo būti apgauta sukčių, nes žinojo, kad jokių prekių ji nėra užsisakiusi, todėl iškart paskambino į banką ginčydama Operacijas, vis dėlto ši pareiškėjos nurodyta aplinkybė, kaip matyti iš ginčo nagrinėjimo metu nustatytų duomenų, nesudarė pagrindo abejoti trečiųjų asmenų galimai siųstu suklastotu Lietuvos pašto pranešimu su prašymu atlikti mokėjimą už pareiškėjos vardu gautą siuntą, kurios pareiškėja pripažįsta neužsakiusi. Be to, kaip nurodo atsiliepiame bankas, pareiškėja neatkreipė dėmesio į tai, kad iš banko SMS žinute gavo *Apple Pay* aktyvavimo kodą, nors pati naudoja *Android* įrenginiu. Duomenų, kad pareiškėja būtų anksčiau tokiu būdu atsiskaičiusi už iš Lietuvos pašto gautus siuntinius, ginčo byloje taip pat nėra. Nurodytos aplinkybės leidžia teigti, kad pareiškėja būtų dėl savo didelio neatsargumo neišsaugojo jos vardu išduotos Kortelės duomenų konfidencialumo – nesiėmė tų saugumo priemonių, kurių privalėjo imtis, kad būtų tinkamai apsaugoti jai suteiktos mokėjimo priemonės duomenys, bei tretiesiems asmenims suteikė vienkartinį saugos kodą, kurį gavo į jai priklausantį telefono numerį trumpąja SMS žinute.

Todėl, konstatavus, kad pareiškėja, nesilaikydama jai, kaip mokėtojai, 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 gražinti (kompensuoti) pareiškėjai neautorizuotos Operacijos lėšų.

Dėl mokėjimo nurodymo neatšaukiamumo

Pareiškėja kreipimesi, be kita ko, nurodė, kad kreipėsi į banką, kai Operacijos lėšos iš jos Kortelės sąskaitos dar nebuvo nurašytos, o tik rezervuotos, todėl bankas turėjo galimybę sustabdyti Operacijos įvykdymą.

Vertinant galimybę atšaukti pareiškėjos vardu pateiktą mokėjimo nurodymą įvykdyti Operaciją, papildomai pažymėtina, kad, vadovaujantis Mokėjimų įstatymo 44 straipsnio 1 dalimi, 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 gražinimas 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 atsiliepiame 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 Kortelės 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 nebuvo nustatytos, t. y. pareiškėja į banką su prašymu atšaukti mokėjimo nurodymą įvykdyti Operaciją (Operacijas) ir (arba) grąžinti šio (-ių) mokėjimo (-ų) lėšas į pareiškėjos Kortelės sąskaitą paskambino po to, kai Operacija (-os) jau buvo įvykdyta (-os), taigi ir Mokėjimų įstatyme bei šalių susitarime nustatytas terminas atšaukti mokėjimo nurodymus jau buvo praėjęs, ir bankas neturėjo jokių galimybių Operaciją (-as) atšaukti.

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

Dėl lėšų grąžinimo procedūros inicijavimo pagal Mastercard mokėjimo kortelių organizacijos taisykles

Papildomos galimybės mokėjimo kortelės turėtoji 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 taikymo⁴. 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 pareiškėjos 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 išvardytą sąrašą⁵. 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 ir buvo įvykdyta Operacija.

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

Todėl, įvertinus visa tai, kas išdėstyta pirmiau, ir nustačius, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, darytina išvada, kad pareiškėjos banko atžvilgiu keliamas reikalavimas grąžinti ir (arba) kompensuoti Operacijos sumą – 265 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

⁴ Teisės aktai nereglamentuoja, kokiomis sąlygomis turi būti vykdomos tokios lėšų grąžinimo procedūros, nes tai nustato konkreiti mokėjimo kortelių organizacija savo parengtose lėšų grąžinimo (angl. *chargeback*) taisyklėse.

⁵ 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.“

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 pareiškėjos 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.

Teisės taikymo ir teisėkūros skyriaus vadovė,
pavadojanti departamento direktorių

Eglė Lukošienė