# LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

## SPRENDIMAS DĖL X. X. IR *REVOLUT BANK UAB* GINČO NAGRINĖJIMO

2022-11-03 Nr. 429-549
Vilnius

Lietuvos bankas gavo X. X. (toliau – pareiškėja) kreipimąsi, kuriuo prašoma išnagrinėti tarp pareiškėjos ir *Revolut Bank UAB* (buvusi *Revolut Payments UAB*[1]) (toliau – bankas) kilusį ginčą.

N u s t a t y t a:

2020 m. rugsėjo 1 d. pareiškėja ir bankas sudarė mokėjimo paslaugų teikimo sutartį (toliau – Sutartis), kurios pagrindu pareiškėjai buvo atidaryta mokėjimo sąskaita Nr. (*duomenys neskelbiami*) (toliau – sąskaita) ir išduota su šia sąskaita susieta „MasterCard" mokėjimo kortelė Nr. (*duomenys neskelbiami*) (toliau – kortelė).

2022 m. liepos 21 d. kortelė buvo pridėta prie mobiliųjų mokėjimų sistemos „Apple Pay" (toliau – *Apple Pay* sistema).

2022 m. liepos 22 d. 9 val. 27 min. ir 9 val. 29 min. per *Apple Pay* sistemą kortele buvo atitinkamai inicijuotos 74,008 JOD (ekv. 103.09 EUR) ir 112,50 JOD (ekv. 156.69 EUR) mokėjimo operacijos (toliau – ginčijamos mokėjimo operacijos) galimai Jordanijoje veikiančiam prekybininkui „Ahl Aljoud Rest" (toliau – gavėjas). Ginčijamų mokėjimo operacijų sumos buvo iš karto rezervuotos pareiškėjos sąskaitoje.

Tą pačią dieną, t. y. liepos 22 d., 19 val. 56 min. pareiškėja kreipėsi į banką, informavo, kad iš jos apgaulės būdu buvo išvilioti kortelės duomenys ir panaudoti ginčijamoms mokėjimo operacijoms inicijuoti, ir prašė atšaukti šių mokėjimo operacijų vykdymą. Pareiškėja pabrėžė, kad ginčijamų mokėjimo operacijų inicijavimo metu buvusi Rumunijoje ir negalėjusi atlikti jokių mokėjimų Jordanijoje. Bendraudama su banku, pareiškėja paaiškino, kad 2022 m. liepos 21 d. elektroniniu paštu gavo laišką iš pašto paslaugų teikėjo, informuojantį, kad pareiškėjai bus pristatytas siuntinys ir ji turi sumokėti siuntinio pristatymo mokestį (iš viso 5 RON). Paspaudusi elektroniniame laiške pateiktą nuorodą, pareiškėja suvedė savo kortelės duomenis, kad apmokėtų siuntinio pristatymo mokestį. Pareiškėja nurodė bandžiusi sumokėti minėtą mokestį du kartus, patvirtindama šiuos mokėjimus į savo telefono numerį banko SMS žinutėmis siųstais vienkartiniais saugos kodais, tačiau atlikti šių mokėjimų jai vis tiek nepavyko. Bankas pranešė pareiškėjai, kad užblokavo jos kortelę, ir informavo, kad jei per 8 dienas nebus gautas gavėjo patvirtinimas apie galutinį atsiskaitymą, pareiškėjos sąskaitoje atlikta lėšų rezervacija bus panaikinta. Atsižvelgdamas į pareiškėjos patiriamus nepatogumus, bankas geranoriškai pasiūlė suteikti pareiškėjai galimybę du mėnesius nemokamai naudotis paslaugų planu „Premium", tačiau pareiškėja šio pasiūlymo atsisakė, nurodydama, kad tenori susigrąžinti ginčijamų mokėjimo operacijų sumas. Paprašyta banko, pareiškėja tą pačią dieną užpildė ir pateikė bankui nustatytos formos prašymą dėl tarptautinės kortelių organizacijos „MasterCard" (toliau – *MasterCard* organizacija) lėšų grąžinimo procedūros (angl. *chargeback*) inicijavimo.

2022 m. liepos 25 d. bankas informavo pareiškėją, kad netenkins pareiškėjos prašymo inicijuoti *MasterCard* organizacijos lėšų grąžinimo procedūrą. Bankas paaiškino pareiškėjai, kad, nustačius, kad ginčijamos mokėjimo operacijos buvo inicijuotos per *Apple Pay* sistemą ir kortelės pridėjimas prie šios sistemos buvo patvirtintas pareiškėjai banko SMS žinute siųstu vienkartiniu saugos kodu, lėšų grąžinimo procedūra yra negalima.

Nesutikdama su banko sprendimu, pareiškėja kreipėsi į Lietuvos banką dėl kilusio vartojimo ginčo nagrinėjimo. Pareiškėja prašė Lietuvos banko rekomenduoti bankui grąžinti (kompensuoti)

[1] *Revolut Payments UAB* buvo reorganizuota, ją prijungiant prie *Revolut Bank UAB*, todėl nuo 2022 m. liepos 1 d. *Revolut Payments UAB* teisės ir pareigos pagal jos sudarytas galiojančias finansinių paslaugų ir kitas sutartis, įskaitant iš šių sutarčių kilusius ginčus, perėjo *Revolut Bank UAB*.

jai ginčijamų mokėjimo operacijų sumas. Pareiškėjos teigimu, ji gavo iš banko SMS žinutę, informuojančią, kad jos kortelė buvo užblokuota dėl pastebėtos įtartinos 50 EUR mokėjimo operacijos, patvirtino tokį kortelės blokavimą ir tuomet pastebėjo, kad kelios minutės iki minėtos banko SMS žinutės iš banko gavimo jos sąskaitoje buvo inicijuotos ginčijamos mokėjimo operacijos. Pareiškėja nurodė neatlikusi ginčijamų mokėjimo operacijų, nežinanti, kaip jos galėjo būti inicijuotos, bet mananti, kad jos inicijuotos sukčiavimo būdu. Pareiškėja papildomai pabrėžė, kad ginčijamos mokėjimo operacijos buvo atliktos Jordanijoje esančiame restorane, nors pareiškėja tuo metu buvo namie Rumunijoje.

Atsiliepime į pareiškėjos kreipimąsi bankas nurodė nesutinkantis su pareiškėjos reikalavimu ir prašė jį atmesti. Banko teigimu, ginčijamos mokėjimo operacijos buvo atliktos ir autorizuotos per *Apple Pay* sistemą, įrenginį, kuriame įdiegta Apple Pay sistema, fiziškai pridėjus prie bekontakčio skaitytuvo. Bankas paaiškino, kad, norint pridėti mokėjimo kortelę prie *Apple Pay* sistemos, reikia ne tik šioje sistemoje nuskenuoti mokėjimo kortelę arba rankiniu būdu įvesti mokėjimo kortelės duomenis (numerį, galiojimo datą, kortelės saugos kodą CVV), bet ir, tai padarius, patvirtinti mokėjimo kortelės pridėjimą prie šios sistemos, įvedant banko SMS žinute į kliento telefono numerį, kurį klientas nurodo ir patvirtina bankui sudarant mokėjimo sutartį, siųstą vienkartinį saugos kodą. Bankas pabrėžė, kad nesuvedus vienkartinio saugos kodo kortelės pridėjimas prie *Apple Pay* sistemos nebūtų buvęs patvirtintas ir atsiskaitymas per *Apple Pay* sistemą būtų neįmanomas, taip pat papildomai paaiškino, kad, jei vienkartinis saugos kodas būtų įvestas neteisingai, kortelės pridėjimo prie *Apple Pay* sistemos procesas būtų kartojamas iš naujo, t. y. vėl reikėtų nuskenuoti kortelę arba rankiniu būdu suvesti pirmiau nurodytus kortelės duomenis, gauti naują vienkartinį saugos kodą, o tada jį suvesti, taip patvirtinant kortelės pridėjimą prie *Apple Pay* sistemos. Banko vidaus sistemų duomenimis, pridedant pareiškėjos kortelę prie *Apple Pay* sistemos, buvo suvesti teisingi kortelės duomenys ir teisingas vienkartinis saugos kodas, kurį bankas SMS žinute siuntė į pareiškėjos telefono numerį (*duomenys neskelbiami*) (toliau – telefono numeris).

Bankas neteigė, kad įrenginys, naudotas pridėti kortelę prie *Apple Pay* sistemos ir per šią sistemą inicijuoti ginčijamą mokėjimo operaciją, priklausė pareiškėjai, tačiau dar kartą pabrėžė, kad be aktyvaus pareiškėjos dalyvavimo, t. y. kortelės duomenų ir vienkartinio saugos kodo atskleidimo, tretieji asmenys nebūtų galėję pridėti pareiškėjos kortelės prie *Apple Pay* sistemos ir vėliau per šią sistemą inicijuoti ginčijamų mokėjimo operacijų. Bankas atkreipė dėmesį, kad, bendraudama su banku, pareiškėja pripažino gavusi ir spaudusi jai tariamo pašto paslaugų teikėjo elektroniniu laišku siųstą nuorodą, atskleidusi savo kortelės duomenis, gavusi ir suvedusi banko jai SMS žinute siųstą vienkartinį saugos kodą (tai patvirtinantys įrodymai pateikti). Bankas taip pat pažymėjo, kad SMS žinute, kuria pareiškėjai buvo siųstas vienkartinis saugos kodas, bankas aiškiai įspėjo pareiškėją, kad šiuo kodu negalima dalintis su kitais asmenimis, tačiau pareiškėja tokio įspėjimo nepaisė ir šį kodą atskleidė tretiesiems asmenims.

Komentuodamas atsisakymo inicijuoti *MasterCard* organizacijos lėšų grąžinimo procedūrą priežastis, bankas paaiškino, kad *MasterCard* organizacija nenustato galimybės ginčyti mokėjimo operacijos tuo pagrindu, kad ji buvo atlikta dėl sukčiavimo, kai mokėjimo kortelės turėtojas dalyvavo vykdant mokėjimo operaciją. Kadangi pareiškėja autorizavo kortelės pridėjimą prie *Apple Pay* sistemos ir (arba) aktyviais savo veiksmais, t. y. pati patvirtino arba perdavė vienkartinį saugos kodą tretiesiems asmenims, kad šie patvirtintų kortelės pridėjimą prie *Apple Pay* sistemos, bankas teigė neturėjęs teisės inicijuoti *MasterCard* organizacijos lėšų grąžinimo procedūros.

Nors ir laiko ginčijamas mokėjimo operacijas tinkamai autorizuotomis pačios pareiškėjos, bankas papildomai nurodė manantis, kad nagrinėjamoje situacijoje pareiškėja, atskleisdama tretiesiems asmenims kortelės duomenis ir vienkartiniu saugos kodu pati patvirtinusi kortelės pridėjimą prie *Apple Pay* sistemos ir (arba) perduodama šį vienkartinį saugos kodą tretiesiems asmenims, taip sudarydama galimybę šiems asmenims patvirtinti kortelės pridėjimą prie *Apple Pay* sistemos, elgėsi itin neatsargiai ir nesilaikydama Lietuvos Respublikos mokėjimų įstatymo 34 straipsnyje ir Sutarties 9 punkte pareiškėjui nustatytų pareigų, susijusių su kortelės ir jos duomenų naudojimu bei saugojimu.

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

Vadovaujantis Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių, patvirtintų Lietuvos banko valdybos 2012 m. sausio 26 d. nutarimu Nr. 03-23, 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. Lietuvos bankas ginčo nagrinėjimo proceso metu neatlieka Lietuvos Respublikos Lietuvos banko įstatymo $42^1$ straipsnyje reglamentuotų patikrinimų, skirtų faktinėms aplinkybėms, susijusioms su Lietuvos banko priežiūrimo finansų rinkos dalyvio galimu Lietuvos banko kompetencijai priskirtų teisės aktų reikalavimų pažeidimu, nustatyti ir įvertinti. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą ir jo pagrindu priima sprendimą.

Pareiškėjos ir banko ginčas kilo dėl banko atsisakymo grąžinti (kompensuoti) pareiškėjai ginčijamų mokėjimo operacijų sumas, kurių bendrą vertė 186,508 JOD (ekv. 259,78 EUR), pagrįstumo.

Pareiškėja savo reikalavimą grąžinti (kompensuoti) ginčijamų mokėjimo operacijų sumas argumentavo tuo, kad šios mokėjimo operacijos buvo įvykdytos be jos žinios ir sutikimo. Bankas teigė, kad ginčijamos mokėjimo operacijos buvo autorizuotos šalių sutartu būdu, atliktos per *Apple Pay* sistemą, prie kurios naudojantis tik pareiškėjai žinomu vienkartiniu saugos kodu buvo pridėta ir patvirtina pareiškėjos kortelė, todėl bankas neturi pareigos savo lėšomis kompensuoti pareiškėjai ginčijamų mokėjimo operacijų sumų.

Šalių ginčas kilo iš jas siejančių mokėjimo paslaugų teikimo santykių. 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 Mokėjimų įstatymas.

Siekiant išspręsti tarp pareiškėjos ir banko kilusį ginčą, Lietuvos banko vertinimu, būtina nustatyti, ar ginčijamos mokėjimo operacijos laikytinos autorizuotomis ir (ar) bankas turėjo (turi) pareigą grąžinti (kompensuoti) pareiškėjai jų sumas.

Kreipdamasi į Lietuvos banką dėl tarp šalių kilusio ginčo nagrinėjimo, pareiškėja neprašė Lietuvos banko rekomenduoti bankui inicijuoti MasterCard organizacijos lėšų grąžinimo procedūros ir nekėlė bankui kitų, su čia procedūra tiesiogiai susijusių, reikalavimų ir (arba) prieštaravimų, todėl banko atsiliepime nurodytos aplinkybės, susijusios su *MasterCard* organizacijos lėšų grąžinimo procedūros negalimumu, šiame sprendime nebus plačiau analizuojamos.

*1. Dėl ginčijamų mokėjimo operacijų autorizavimo*

Mokėjimų įstatymo 29 straipsnio 1 dalyje nustatyta, kad mokėjimo operacija laikoma autorizuota tik tada, kai mokėtojas duoda sutikimą ją vykdyti. Mokėtojas gali duoti sutikimą įvykdyti vieną arba kelias mokėjimo operacijas. Sutikimas gali būti duodamas ir per lėšų gavėją. Jei sutikimo nėra, laikoma, kad mokėjimo operacija yra neautorizuota (Mokėjimų įstatymo 29 straipsnio 2 dalis). Vadovaujantis Mokėjimų įstatymo 13 straipsnio 3 dalies 3 punktu ir 29 straipsnio 1 punktu, sutikimo davimo sąlygos ir tvarka turi būti aptartos mokėtojo ir jo mokėjimo paslaugų teikėjo sudaromoje mokėjimo paslaugų teikimo sutartyje.

Ginčo nagrinėjimo metu nustatyta, kad ginčijamos mokėjimo operacijos buvo atliktos per *Apple Pay* sistemą, prie kurios buvo pridėta pareiškėjos kortelė. Bankas nurodė, kad kortelės pridėjimas prie *Apple Pay* sistemos buvo patvirtintas vienkartiniu saugos kodu, kurį bankas SMS žinute siuntė į pareiškėjos telefono numerį. Bankas pateikė SMS žinutės su vienkartiniu saugos kodu išsiuntimą pareiškėjai patvirtinančius įrodymus. Nors kreipimesi į Lietuvos banką pareiškėja šių aplinkybių niekaip nepakomentavo ir netgi priešingai – teigė nežinojusi, kaip ginčijamos mokėjimo operacijos galėjo būti inicijuotos, iš banko Lietuvos bankui pateiktų banko ir pareiškėjos susirašinėjimo kopijų matyti, kad pareiškėja ne tik neneigė gavusi iš banko SMS žinutę su vienkartiniu saugos kodu ir naudojusi šį kodą, bet ir savo iniciatyva pateikė bankui savo įrenginio ekrano nuotrauką, patvirtinančią šios SMS žinutės gavimą.

Banko teigimu, kortelės pridėjimas prie *Apple Pay* sistemos, patvirtinant tokį pridėjimą vienkartiniu saugos kodu, nepaisant to, kas faktiškai pridėjo kortelę prie *Apple Pay* sistemos (pati pareiškėja ar trečiasis asmuo, kuriam pareiškėja perdavė tam reikalingus duomenis), remiantis Sutarties 14 punktu, laikomas pareiškėjos sutikimo vykdyti kortele per *Apple Pay* sistemą inicijuotas mokėjimo operacijas davimu. Minėtame Sutarties punkte nustatyta, kad: „Mokėjimus atlikti ir išgryninti pinigų taip pat galite naudodamiesi „Revolut" kortele. Tai galite padaryti įvesdami savo „Revolut" kortelės duomenis (kortelės numerį, galiojimo datą ir CVC numerį) arba PIN kodą. <…> Sutikimą atlikti mokėjimus savo „Revolut" kortele taip pat duodate: <…> pateikdami „Revolut" kortelės numerį ir kitą informaciją prekybininkui ar paslaugų teikėjui ir patvirtindami šį mokėjimą naudojant „3D Secure" metodą <…>". Remdamasis Sutarties 14 punktu ir vidaus sistemų duomenimis, kurie patvirtina, kad bankas pareiškėjos telefono numeriu 2022 m. liepos 21 d. siuntė SMS žinutę su vienkartiniu saugos kodu, skirtu kortelės pridėjimui prie *Apple*

*Pay* sistemos patvirtinti, netrukus po to kortelės pridėjimas prie šios sistemos buvo patvirtintas šiuo kodu ir 2022 m. liepos 22 d. ginčijamos mokėjimo operacijos buvo inicijuotos per *Apple Pay* sistemą, bankas laiko ginčijamas mokėjimo operacijas autorizuotomis pačios pareiškėjos.

Kaip matyti, darydamas pirmiau nurodytas išvadas, bankas iš esmės rėmėsi tik jo vidaus sistemose užfiksuotais įvykiais ir jų atitikmeniu Sutartyje bendrais bruožais apibrėžtiems sutikimo vykdyti mokėjimo operacijas davimo kriterijais, neatsižvelgdamas į pareiškėjos bankui nurodytas kortelės duomenų atskleidimo tretiesiems asmenims aplinkybes ir atskirai nevertindamas ginčijamų mokėjimo operacijų inicijavimo aplinkybių (pvz., kaip ir kada ir gavėjas gavo kortelės duomenis ir (arba) sutikimą jų pagrindu inicijuoti ginčijamas mokėjimo operacijas), nors būtent šios aplinkybės, Lietuvos banko nuomone, turi esminės reikšmės, vertinant, ar ginčijamos mokėjimo operacijos laikytinos autorizuotomis.

Mokėjimo operacijų autorizuotumo klausimai negali būti vertinami izoliuotai, t. y. vien tik remiantis faktu, kad mokėtojo veiksmai formaliai atitinka mokėtojo ir mokėjimo paslaugų teikėjo sutartus sutikimo vykdyti mokėjimo operacijas davimo kriterijus, ypač tada, kai turima duomenų, kad mokėtojas, nors ir atliko šiuos veiksmus, tačiau galimai nesuprato, kad tokiais savo veiksmais sudaro galimybę tretiesiems asmenims inicijuoti mokėjimo operacijas, kurių mokėtojas nesiekė atlikti. Vadovaujantis Mokėjimų įstatymo 37 straipsnio 3 dalimi, mokėtojo mokėjimo paslaugų teikėjo užregistruotas mokėjimo priemonės (nagrinėjamu atveju – kortelės) naudojimas nebūtinai yra pakankamas įrodymas, kad mokėtojas autorizavo mokėjimo operaciją. Taigi, vien aplinkybė, kad banko vidaus sistemose buvo užfiksuota, kad, atliekant ginčijamas mokėjimo operacijas, buvo panaudoti pareiškėjo kortelės duomenys ir (arba) kad bankas buvo siuntęs pareiškėjui vienkartinį saugos kodą, kuris buvo panaudotas pridedant kortelę prie *Apple Pay* sistemos, savaime neįrodo, kad ginčijama mokėjimo operacija buvo atlikta esant pareiškėjo valiai ir sutikimui, kaip jis suprantamas Mokėjimų įstatymo 29 straipsnio 1 dalyje.

Pažymėtina, kad valia yra esminis kiekvieno sandorio, kaip teisinio veiksmo, kuriuo siekiama sukurti tam tikras teises ir pareigas, elementas[2]. Taigi, mokėtojo valia atlikti konkrečią mokėjimo operaciją taip pat yra viena iš esminių aplinkybių, į kurią turėtų būti atsižvelgta, vertinant, ar mokėjimo operacija, kurios autorizuotumą mokėtojas ginčija, laikytina autorizuota. Mokėtojo valios išraiškos forma turėtų būti vertinama, atsižvelgiant į ją atspindinčių ir pagrindžiančių ginčijamų mokėjimo operacijų inicijavimo ir vykdymo aplinkybių bei šias aplinkybes pagrindžiančių ir (arba) paneigiančių įrodymų visumą.

Iš banko pateiktų vidaus sistemų išrašų kopijų, matyti, kad sutartinių santykių su banku metu pareiškėja naudojosi *Apple Pay* sistema iš skirtingų jai priklausančių įrenginių[3], tačiau 2022 m. liepos 21 d. kortelė prie *Apple Pay* sistemos buvo pridėta ir 2022 m. liepos 22 d. ginčijamos mokėjimo operacijos per šią sistemą buvo inicijuotos iš įrenginio, kurio pareiškėja iki tol nebuvo naudojusi (toliau – naujas *iPhone* įrenginys). Byloje neturima duomenų, kurie leistų teigti, kad naujas *iPhone* įrenginys galėjo priklausyti pareiškėjai ir (arba) būti jos žinioje. Savo atsiliepime bankas taip pat neteigė ir neįrodinėjo, kad naujas *Iphone* įrenginys galėjo priklausyti pareiškėjai.

Bankas nurodė, kad ginčijamos mokėjimo operacijos buvo inicijuotos fiziškai pridėjus naują *Iphone* įrenginį prie bekontakčio skaitytuvo. Banko pateiktose ginčijamų mokėjimo operacijų išrašų kopijose nurodyta, kad gavėjo veikla priklauso restoranų ir maitinimo vietų veiklos kategorijai[4], o gavėjo fizinės veiklos vieta yra Jordanijos sostinėje Amane. Bankas paaiškino, kad kartu su inicijuotomis mokėjimo operacijomis pateikti lėšų gavėjų duomenys kartais gali nesutapti su tais duomenimis, kuriuos klientai mato įsigydami iš gavėjų prekes ar paslaugas, tačiau įrodymų, kad ginčijamų mokėjimo operacijų atžvilgiu būtent taip ir galėjo nutikti, nepateikė. Taigi, pagrindo teigti, kad kartu su mokėjimo nurodymais dėl ginčijamų mokėjimo operacijų vykdymo bankui pateikti gavėjo, įskaitant jo veiklos vietą, duomenys neatitinka faktinių gavėjo duomenų ir (arba) kad naujas *iPhone* įrenginys prie bekontakčio skaitytuvo buvo pridėtas kitoje, negu pirmiau nurodytoje gavėjo veiklos vietoje, Lietuvos bankas neturi. Tai, kad naujas *iPhone* įrenginys galėjo būti fiziškai pridėtas prie bekontakčio skaitytuvo gavėjo nurodytoje veiklos vietoje Jordanijoje, Lietuvos banko nuomone, liudija ir tai, kad ginčijamos mokėjimo operacijos buvo inicijuotos Jordanijos nacionaline valiuta (JOD).

Iš bylos duomenų matyti, kad pareiškėja gyvena Rumunijoje. Duomenų, kad ginčijamų mokėjimo operacijų inicijavimo metu pareiškėja galėjo būti Jordanijoje, neturima. Priešingai,

---

[2] „Apgaulės atveju sudarytas sandoris yra ne sandorio šalies laisvos valios išraiškos rezultatas, o kitos sandorio šalies ar trečiojo asmens nesąžiningų veiksmų rezultatas. Jeigu apgaulės nebūtų buvę, apgautoji sandorio šalis sandorio arba apskritai nebūtų sudariusi, arba būtų sudariusi jį visiškai kitokiomis sąlygomis.“ (Lietuvos Aukščiausiojo Teismo 2016 m. gegužės 12 d. nutartis civilinėje byloje Nr. 3K-3-268-421/2016).

[3] Banko vidaus sistemose užfiksuoti šie pareiškėjai naudoti įrenginiai: (*duomenys neskelbiami*).

[4] Prekybininko kategorijos kodas (angl. Merchant Category Code) yra 5812.

pareiškėja teigė, kad tuo metu buvo namie Rumunijoje ir negalėjo atlikti ginčijamų mokėjimo operacijų Jordanijoje. Įrodymų, kurie galėtų paneigti pareiškėjos nurodytas aplinkybes, bankas nepateikė.

Remiantis pareiškėjos bankui teikta informacija, pareiškėja 2022 m. liepos 21 d. elektroniniu paštu gavo laišką iš, kaip ji manė, pašto paslaugų teikėjo Poșta Română S. A., ir paspaudusi šiame laiške pateiktą nuorodą, atsidariusiame lange suvedė kortelės duomenis ir banko siųstą vienkartinį saugos kodą, turėdama tikslą kortele sumokėti 5 RON dydžio siuntinio pristatymo mokestį. Taigi, perduodama savo kortelės duomenis, pareiškėja, kaip ji teigė, aktyviais veiksmais siekė atlikti 5 RON mokėjimą, o ne ginčijamas mokėjimo operacijas. Pareiškėja teigė, kad gavėjo nežino ir jo fizinėje veiklos vietoje nėra buvusi. Byloje nėra duomenų, kurie leistų teigti, kad pareiškėja savo ar kitų asmenų naudai būtų siekusi įsigyti ir (arba) būtų įsigijusi iš gavėjo prekes ar paslaugas ir, siekdama atsiskaityti už jas, galėjo būti perdavusi gavėjui savo kortelės duomenis, įskaitant sutikimą naudoti juos ginčijamoms mokėjimo operacijoms inicijuoti. Duomenų, kad po ginčijamų mokėjimo operacijų įvykdymo gavėjas būtų suteikęs pareiškėjai ar jos nurodytiems asmenims kokias nors prekes ir (arba) paslaugas, taip pat nėra. Įrodymų, kurie galėtų paneigti pareiškėjos nurodytas aplinkybes, bankas taip pat nepateikė. Taigi, remiantis byloje turimais duomenimis, pagrindo teigti, kad pareiškėja galėjo tiesiogiai kontaktuoti su gavėju, perduoti jam savo kortelės duomenis ir (arba) kitu būdu duoti jam sutikimą inicijuoti ginčijamas mokėjimo operacijas, Lietuvos bankas neturi. Priešingai, byloje turimi duomenys leidžia daryti išvadą, kad kortelės duomenys, kaip ir nurodė pareiškėja, galėjo būti išvilioti iš jos apgaulės būdu, siekiant juos panaudoti neteisėtais tikslais, t. y. pasisavinti lėšas iš pareiškėjos sąskaitos. Pirma, pareiškėjai buvo atsiųstas elektroninis laiškas su nuoroda, kurį siuntė ne gavėjas, o tariamas pašto paslaugų teikėjas. Kaip nurodyta pirmiau, suklaidinta tariamo pašto paslaugų teikėjo pareiškėja manė, kad turi sumokėti šiam paslaugų teikėjui 5 RON (ekv. 1,02 EUR) pristatymo mokestį. Byloje neturima duomenų, kad pareiškėjai būtų pavykę kortele atlikti minėtą 5 RON mokėjimą ir (arba) kad ginčijamos mokėjimo operacijos būtų buvusios inicijuotos kitokiomis, negu pareiškėja pirmiau nurodė, aplinkybėmis, t. y. buvo inicijuotos ne dėl to ir ne po to, kai pareiškėja, suklaidinta tariamo pašto paslaugų teikėjo, bandė kortele sumokėti siuntinio pristatymo mokestį. Antra, kaip konstatuota pirmiau, byloje nėra duomenų, leidžiančių teigti, kad naujas *iPhone* įrenginys galėjo priklausyti pareiškėjai ir (arba) būti jos žinioje, taip pat, kad pareiškėja ginčijamų mokėjimo operacijų inicijavimo metu galėjo būti gavėjo fizinėje veiklos vietoje, kuri galimai Jordanijoje, o ne Rumunijoje, kurioje gyvena pareiškėja, ir fiziškai pridėti ir (arba) dalyvauti pridedant naują *iPhone* įrenginį prie bekontakčio skaitytuvo, taip leidžiant inicijuoti ginčijamas mokėjimo operacijas. Trečia, iš byloje turimų duomenų matyti, kad panašiu, kaip ir ginčijamų mokėjimo operacijų inicijavimo, laikotarpiu, panaudojant kortelės duomenis buvo bandoma inicijuoti ir 50 EUR mokėjimą kriptoturto keityklai „MoonPay“, kurio pareiškėja teigė taip pat neatlikusi. Pastarasis mokėjimas nebuvo įvykdytas.

Pažymėtina ir tai, kad tiek Mokėjimų įstatymo 29 straipsnio 1 dalyje, tiek Sutarties 14 punkte aiškiai įvardyta, kad veiksmus, kurie pareiškėjo, kaip mokėtojo, ir banko, kaip mokėtojo mokėjimo paslaugų teikėjo, susitarimu reikš sutikimo vykdyti mokėjimo operacijas davimu, aktyviais veiksmais turi atlikti pats pareiškėjas. Kaip ir nurodyta pirmiau, bankas pateikė įrodymus, patvirtinančius, kad ginčijamos mokėjimo operacijos buvo inicijuotos pagal pareiškėjos kortelės duomenis ir kad iki ginčijamų mokėjimo operacijų inicijavimo pareiškėjos kortelė buvo pridėta panaudojant vienkartinį saugos kodą, kuris buvo išsiųstas pareiškėjos telefono numeriu, tačiau įrodymų, kurie patvirtintų, kad vienkartinį saugos kodą pridėdama kortelę prie *Apple Pay* sistemos panaudojo, kortelės duomenis gavėjui perdavė ir (arba) kitu būdu savo sutikimą inicijuoti ginčijamas mokėjimo operacijas gavėjui davė pati pareiškėja, nepateikė. Lietuvos banko vertinimu, esant duomenų, kad mokėtojui išduota mokėjimo priemone ir (arba) jos duomenimis galėjo būti pasinaudota neteisėtai, t. y. tam, kad iš mokėtojo mokėjimo sąskaitos būtų atliktos mokėjimo operacijos, ir neturint objektyvių ir pakankamų įrodymų, kad šios mokėjimo operacijos atliktos esant mokėtojo valiai ir sutikimui, tokios mokėjimo operacijos negalėtų būti laikomis autorizuotomis.

Įvertinęs ginčo šalių pateiktus paaiškinimus ir įrodymus, Lietuvos bankas nenustatė objektyvių ir pakankamų pagrindų, leidžiančių teigti, kad ginčijamos mokėjimo operacijos buvo įvykdytos esant pareiškėjos valiai ir sutikimui, kaip jis suprantamas Mokėjimų įstatymo 29 straipsnio dalies kontekste, todėl laiko ginčijamas mokėjimo operacijas neautorizuotomis.

*2. Dėl neautorizuotų ginčijamos mokėjimo operacijų pasekmių ir pareiškėjos teisės į šių mokėjimo operacijų sumų grąžinimą*

Vadovaujantis Mokėjimų įstatymo 38 straipsnio 1 dalimi, nesant Mokėjimų įstatymo 39 straipsnio 1 ir 3 dalyje nustatytų aplinkybių, mokėtojo mokėjimo paslaugų teikėjas privalo grąžinti mokėtojui visą neautorizuotos mokėjimo operacijos sumą ne vėliau kaip iki 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). 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 to paties įstatymo 34 straipsnyje nustatytų pareigų, susijusių su mokėjimo priemonėmis ir personalizuotais saugumo duomenimis (Mokėjimų įstatymo 39 straipsnio 3 dalis). Mokėjimų įstatymo 34 straipsnis nustato mokėtojui, kuriam išduota mokėjimo priemonė, pareigą naudotis šia mokėjimo priemone pagal jos išdavimą ir naudojimą reglamentuojančias sąlygas, o sužinojus apie jos praradimą, vagystę arba neteisėtą pasisavinimą ar neautorizuotą jos naudojimą, nedelsiant apie tai pranešti mokėjimo paslaugų teikėjui arba jo nurodytam subjektui (Mokėjimų įstatymo 34 straipsnio 1 dalis), taip pat, gavus mokėjimo priemonę, imtis veiksmų, kad būtų apsaugoti personalizuoti saugumo duomenys (Mokėjimų įstatymo 34 straipsnio 2 dalis). Vadovaujantis Mokėjimų įstatymo 37 straipsnio 1 ir 3 dalimis, pareiga įrodyti, kad mokėjimo operacijos autentiškumas buvo patvirtintas, ji buvo tinkamai užregistruota, įrašyta į sąskaitas ir jos nepaveikė techniniai trikdžiai arba kiti mokėjimo paslaugų teikėjo teikiamos paslaugos trūkumai, tenka mokėtojo mokėjimo paslaugų teikėjui. Mokėjimų įstatymo 39 straipsnio 4 dalyje nustatyta, kad, kai mokėtojo mokėjimo paslaugų teikėjas nereikalauja saugesnio autentiškumo patvirtinimo, mokėtojui dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai tenka tik tuo atveju, jeigu jis veikė nesąžiningai.

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 tada, kai įrodomas mokėtojo sukčiavimas (nesąžiningumas arba tyčia) arba didelis neatsargumas (Mokėjimų įstatymo 37 straipsnio 3 dalis ir 39 straipsnio 3 dalis), ir (arba) tik tada, kai mokėtojo mokėjimo paslaugų teikėjas nereikalauja saugesnio autentiškumo patvirtinimo ir nenustatomas pareiškėjo nesąžiningumas (Mokėjimų įstatymo 39 straipsnio 4 dalis).

Byloje neturima duomenų, kad nagrinėjamu atveju pareiškėja galėjo elgtis nesąžiningai ir (arba) tyčia, todėl galimas mokėtojo sukčiavimas, kaip pagrindas atleisti mokėtojo mokėjimo paslaugų teikėją nuo pareigos atlyginti mokėtojui nuostolius dėl neautorizuotos mokėjimo operacijos įvykdymo, šiame sprendime atskirai nebus plačiau analizuojamas.

Byloje turimi duomenys leidžia daryti išvadą, kad nagrinėjamu atveju bankas taikė saugesnio autentiškumo patvirtinimo reikalavimus, t. y. reikalavo, kad kortelės prie *Apple Pay* sistemos pridėjimas būtų patvirtintas vienkartiniu saugos kodu, kuris išsiųstas pareiškėjos telefono numeriu ir turėjo likti žinomas tik pačiai pareiškėjai, ir nesuvedus šio kodo kortelės pridėjimas prie *Apple Pay* sistemos nebūtų buvęs įmanomas, todėl saugesnio autentiškumo patvirtinimo reikalavimų netaikymas, kaip pagrindas taikyti mokėtojo mokėjimo paslaugų teikėjui atsakomybę už nuostolius, atsiradusius dėl neautorizuotos mokėjimo operacijos įvykdymo, šiame sprendime taip pat atskirai nebus plačiau analizuojamas.

Kaip minėta pirmiau, bankas savo sprendimą negrąžinti (nekompensuoti) pareiškėjai ginčijamų mokėjimo operacijų sumų grindžia aplinkybe, kad ginčijamos mokėjimo operacijos buvo tinkamai autorizuotos, t. y. pareiškėjos kortelę, kuria šios mokėjimo operacijos buvo atliktos, prie *Apple Pay* sistemos pridėjus taikant saugesnio autentiškumo patvirtinimo procedūrą, tačiau kartu nurodė, kad pareiškėjos elgesiui būdingas ir didelis neatsargumas. Tai reiškia, kad, atsižvelgiant į pirmiau minėtas Mokėjimų įstatymo nuostatas, taip pat ir į šiuos banko teiginius, siekiant įvertinti, ar bankas pagrįstai atsisakė grąžinti (kompensuoti) pareiškėjai ginčijamų mokėjimo operacijų, kurias Lietuvos bankas, priešingai, nei teigė bankas, vis dėlto laiko neautorizuotomis, sumas ir ar pareiškėjai galėtų būti taikoma Mokėjimų įstatymo 39 straipsnio 3 dalis, būtina nustatyti, ar pareiškėjos elgesys, atskleidžiant kortelės duomenis ir (ar) atliekant kitus veiksmus, dėl kurių galėjo būti įvykdytos ginčijamos mokėjimo operacijos, vertintinas kaip didelis neatsargumas, dėl kurio visi nuostoliai, atsiradę dėl ginčijamų mokėjimo operacijų įvykdymo, turėtų tekti pačiai pareiškėjai.

Mokėtojo neatsargumo laipsnio vertinimas yra susijęs su ginčo byloje nustatytų individualių, specifinių aplinkybių, kurias patvirtina ginčo byloje esantys įrodymai ir (arba) yra šalių neginčijamos neautorizuotos mokėjimo operacijos įvykdymo aplinkybės, visumos vertinimu. Taigi, išvada dėl mokėtojo paprasto ar didelio neatsargumo, kaip vertinamojo pobūdžio aplinkybė, negali būti daroma izoliuotai, išsamiai neįvertinus viso neautorizuotos mokėjimo operacijos

įvykdymo ir su juo susijusių aplinkybių konteksto.

Kriterijai, į kuriuos reikėtų atsižvelgti vertinant kaltės laipsnį, yra iš dalies suformuluoti Antrosios mokėjimo paslaugų direktyvos preambulės 72 punkte: „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 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" (Lietuvos Aukščiausiojo Teismo 2017 m. balandžio 13 d. nutartis civilinėje byloje Nr. e3K-3-180-378/2017, 29 punktas).

Byloje neturima duomenų, kad nagrinėjamam ginčui aktualiu laikotarpiu į banko vidaus sistemas būtų įsilaužta ir (arba) jas būtų paveikę techniniai trikdžiai, dėl kurių pareiškėjos kortelės duomenys ir (arba) pareiškėjai siųstas vienkartinis saugos kodas galėjo tapti žinomas tretiesiems asmenims ir (arba) dėl kurių tretieji asmenys dėl nuo banko priklausančių aplinkybių būtų kitaip įgiję galimybę neteisėtai pasinaudoti pareiškėjos kortele, jos ir (arba) su jos naudojimu susijusiais duomenimis ir (arba) sąskaita. Vadinasi, pirmiau minėti duomenys tretiesiems asmenims turėjo tapti žinomi kitu būdu.

Pirmiau minėtame Mokėjimų įstatymo 34 straipsnyje nustatyta viena iš mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigų – naudotis mokėjimo priemone pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas. Panašias pareigas nustato Sutarties 9 dalis, kurioje nustatyta, kad: „Darome viską, ką galime, kad apsaugotume jūsų pinigus. To paties prašome ir jūsų – saugoti savo saugumo informaciją ir „Revolut" kortelę. Tai reiškia, jog neturėtumėte savo saugumo informacijos laikyti šalia „Revolut" kortelės ir turėtumėte juos paslėpti arba apsaugoti, jei kur nors užsirašote ar laikote. Savo saugumo informacijos nepateikite niekam kitam, išskyrus atvirosios bankininkystės paslaugų teikėją ar trečiosios šalies teikėją, besilaikantį teisės aktų reikalavimų<...>" Taigi, aptartos Sutarties nuostatos aiškiai nustato, kad už mokėjimo priemonės ir personalizuotų saugumo duomenų konfidencialumą yra atsakingas mokėtojas, šiuo atveju – pareiškėja. Atsižvelgiant į tai, manytina, kad pareiškėjos elgesys būtų laikomas atitinkančiu mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, jei būtų nustatyta, kad ji ėmėsi adekvačių veiksmų (arba nuo tam tikrų veiksmų susilaikė), kad būtų tinkamai užtikrintas kortelės ir kitų su jos naudojimu susijusių duomenų, sudarančių sąlygas inicijuoti ir tvirtinti mokėjimus, konfidencialumas.

Prašydama Lietuvos banko išnagrinėti tarp šalių kilusį vartojimo ginčą, pareiškėja neatskleidė Lietuvos bankui kortelės duomenų praradimo fakto ir aplinkybių, teigė apie ginčijamas mokėjimo operacijas sužinojusi tik po to, kai 2022 m. liepos 22 d. gavo iš banko SMS žinutę, informuojančią apie jos kortelės blokavimą, ir nežinojusi, kaip šios mokėjimo operacijos galėjo būti inicijuotos. Vis dėlto, iš bylos duomenų matyti, kad pareiškėjos Lietuvos bankui nurodytos aplinkybės prieštarauja pačios pareiškėjos bankui pirmiau nurodytai informacijai ir ginčo nagrinėjimo metu nustatytoms faktinėms aplinkybėms. Pirma, banko SMS žinutę apie jos kortelės blokavimą ji gavo po to, kai 2022 m. liepos 22 d. kreipėsi į banką dėl pastebėtų jos sąskaitoje inicijuotų ginčijamų mokėjimo operacijų ir banko buvo informuota, kad jos kortelė bus užblokuota. Antra, kaip nurodyta pirmiau, pareiškėja pati nurodė bankui kortelės duomenų atskleidimo ir ginčijamų mokėjimo operacijų inicijavimo aplinkybes, t. y. nurodė, kad kortelės duomenis atskleidė ir kitus veiksmus atliko gavusi iš tariamo pašto paslaugų teikėjo elektroninį laišką, informuojantį apie gautą siuntinį ir prašantį sumokėti siuntinio pristatymo mokestį, ir neneigė, kad gavo ir panaudojo banko jai siųstą vienkartinį saugos kodą, siekdama sumokėti pirmiau nurodytą mokestį. Taigi, byloje turimi duomenys leidžia daryti išvadą, kad kortelės duomenis ir vienkartinį saugos kodą, skirtą pridėti kortelę prie Apple Pay sistemos, tretiesiems asmenims atskleidė pati pareiškėja.

Iš banko pareiškėjai 2022 m. liepos 21 d. siųstos SMS žinutės su vienkartiniu saugos kodu, skirtu kortelės pridėjimui prie *Apple Pay* sistemos patvirtinti, matyti, kad joje buvo nurodyta, kad šis kodas yra skirtas, norint naudotis *Apple Pay* sistema[5]. Minėtoje SMS žinutėje taip pat nurodyta, kad vienkartiniu saugos kodu negalima dalintis su kitais asmenimis. Įvertinus tai, kad, remiantis

[5] Banko siųstos SMS žinutės tekstas originalo kalba: „Revolut: verification code for Apple Pay: (*duomenys neskelbiami*). Never share it with anyone, ever."

byloje turimais duomenimis, iki ginčijamų mokėjimo operacijų inicijavimo pareiškėja naudojosi *Apple Pay* sistema iš jai priklausančių skirtingų įrenginių, darytina išvada, kad pareiškėja turėjo patirties ir žinių, kad galėtų suprasti, kad banko SMS žinute jai siųstas vienkartinis saugos kodas yra skirtas kortelei prie *Apple Pay* sistemos pridėti, o ne konkrečiam mokėjimui atlikti ir patvirtinti, . Lietuvos banko nuomone, pirmiau nurodyta pareiškėjos naudojimosi *Apple Pay* sistema patirtis, taip pat turėjo būti pakankama suprasti, kad, kartą pridėjus kortelę prie *Apple Pay* sistemos ir patvirtinus tokį jos pridėjimą vienkartiniu saugos kodu, bankas pakartotinai neprašys pareiškėjos tvirtinti kiekvieną per šią sistemą inicijuojamą mokėjimo operaciją, laikydamas, kad tokia mokėjimo operacija atlikta esant pareiškėjos sutikimui. Jei pareiškėja, kaip ji pati teigė, atskleisdama kortelės duomenis tariamam pašto paslaugų teikėjui ir atlikdama tolesnius mokėjimus, norėjo atlikti tik vieną konkretų mokėjimą, t. y. sumokėti siuntinio pristatymo mokestį, Lietuvos banko nuomone, pareiškėjai turėjo kilti įtarimų, kodėl, norint atsiskaityti už šią paslaugą, jos prašoma patvirtinti kortelės pridėjimą prie *Apple Pay* sistemos, ypač atsižvelgiant į tai, kad pareiškėja savo įrenginiuose jau buvo pridėjusi kortelę prie Apple Pay sistemos, o 5 RON mokėjimą bandė atlikti ne per šią sistemą. Jei naujas *iPhone* įrenginys, iš kurio kortelė buvo naujai pridėta prie *Apple Pay* sistemos ir vėliau per ją inicijuotos ginčijamos mokėjimo operacijos, nepriklausė pareiškėjai, gavus banko SMS žinutę su vienkartiniu saugos kodu, skirtu kortelei prie *Apple Pay* sistemos pridėti, pareiškėjai taip pat turėjo kilti klausimų, kas, iš kokio įrenginio ir kodėl bando jos kortelę pridėti prie *Apple Pay* sistemos. Byloje neturima duomenų, kad 2022 m. liepos 21 d. gavusi iš banko minėtą SMS žinutę, pareiškėja būtų kreipusis į banką ir mėginusi išsiaiškinti tokios žinutės siuntimo priežastis. Priešingai, kaip matyti iš byloje turimų duomenų, pareiškėja, pažeisdama SMS žinutėje nurodytą draudimą, vis dėlto atskleidė vienkartinį saugos kodą tretiesiems asmenims ir taip galimai sudarė jiems galimybę iš naujo *iPhone* įrenginio pridėti kortelę prie *Apple Pay* sistemos ir vėliau per ją inicijuoti ginčijamas mokėjimo operacijas.

Iš byloje turimų duomenų matyti, kad iki ginčijamų mokėjimo operacijų įvykdymo banko išduota (-omis) mokėjimo kortele (-ėmis) pareiškėja naudojasi nuo 2020 m. rugsėjo mėnesio, o iki tol, t. y. nuo 2018 m. rugpjūčio mėn. naudojosi analogiškomis *Revolut Ltd* paslaugomis. Taigi, pareiškėjos turima naudojimosi mokėjimo kortelėmis patirtis, Lietuvos banko vertinimu, turėjo būti pakankama, kad ji galėtų (turėtų) suprasti, kad kortelės duomenų, SMS žinute gauto vienkartinio saugos kodo atskleidimas ar kitokio autorizavimo veiksmo atlikimas yra sietini su lėšų iš sąskaitos, su kuria susieta kortelė, pervedimu, o pirmiau nurodytų veiksmų atlikimas gali lemti tam tikras teisines pasekmes, t. y. kortelės duomenų praradimą, neteisėtą jų panaudojimą ir (ar) neautorizuotų mokėjimo operacijų iš sąskaitos, su kuria susieta kortelė, įvykdymą.

Net jei pareiškėja, gavusi tariamo pašto paslaugų teikėjo elektroninį laišką su nuoroda, tuo metu nesuprato, kad šiuo elektroniniu laišku iš jos bandoma apgaulės būdu išvilioti kortelės duomenis, ir (arba) nepagalvojo, kad kortelės duomenų atskleidimas gali sukelti jai neigiamų pasekmių, tolesni jos veiksmai, t. y. nereagavimas į banko jai siųstą informaciją ir vienkartinio saugos kodo, skirto kortelei prie Apple Pay sistemos patvirtinti, naudojimas ir (arba) atskleidimas, Lietuvos banko nuomone, rodo pareiškėją buvus itin neatsargią.

Įvertinus ginčo byloje turimus duomenis, darytina išvada, kad nagrinėjamu atveju pareiškėja jai išduota kortele ir su ja susijusiais duomenimis, įskaitant vienkartinį saugos kodą, naudojosi nesilaikydama kortelės išdavimą ir naudojimą reglamentuojančių sąlygų ir nevykdė Mokėjimų įstatymo 34 straipsnyje 1 dalies 1 punkte ir 2 dalyje bei Sutarties 9 punkte jam nustatytų pareigų.

Mokėjimų įstatymo 39 straipsnio 5 dalyje nustatyta, kad mokėtojas neturi patirti jokių nuostolių dėl prarastos, pavogtos ar neteisėtai pasisavintos mokėjimo priemonės po to, kai pateikia šio įstatymo 34 straipsnio 1 dalies 2 punkte nurodytą pranešimą, išskyrus atvejus, kai jis veikė nesąžiningai. Vertinant, ar mokėtojo mokėjimo paslaugų teikėjui, remiantis Mokėjimų įstatymo 39 straipsnio 5 dalies nuostatomis, gali tekti pareiga atlyginti mokėtojui nuostolius, patirtus dėl neautorizuotos mokėjimo operacijos įvykdymo, Lietuvos banko nuomone, būtina atsižvelgti ne tik į Mokėjimų įstatymo 34 straipsnio 1 dalies 2 punkte nurodyto pranešimo apie neautorizuotos mokėjimo operacijos įvykdymą faktą, bet ir į šio pranešimo pateikimo laiką ir aplinkybes, kurios jau buvo faktiškai įvykusios, kai šis pranešimas buvo pateiktas.

Bylos duomenimis, kad prarado kortelės duomenis ir jie buvo panaudoti neautorizuotoms ginčijamoms mokėjimo operacijoms atlikti, pareiškėjas informavo banką po to, kai bankas buvo gavęs mokėjimo nurodymus vykdyti ginčijamas mokėjimo operacijas ir jų pagrindu pareiškėjos sąskaitoje rezervavęs šių mokėjimo operacijų sumą. Duomenų, kurie leistų teigti, kad bankas, priimdamas vykdyti mokėjimo nurodymus atlikti ginčijamas mokėjimo operacijas, galėjo pažeisti Mokėjimų įstatymą, kitus jam taikomus teisės aktus ir (arba) *MasterCard* organizacijos taisykles,

neturima. Objektyvaus pagrindo teigti, kad iki pareiškėjos kreipimosi į banką bankas galėjo (turėjo) suprasti, kad pareiškėja galimai tapo sukčių auka ir ginčijama mokėjimo operacija yra inicijuota be pareiškėjo sutikimo ar žinios, taip pat nėra. Iš bylos duomenų matyti, kad pastarosios aplinkybės bankui tapo žinomos tik po to, kai, bankui priėmus vykdyti mokėjimo nurodymą ir rezervavus lėšas pareiškėjo sąskaitoje, pareiškėja pati jį apie tai informavo. Vėlesnis šių aplinkybių paaiškėjimas nekeičia fakto, kad pareiškėja, nors ir nesiekė ginčijamų mokėjimo operacijų įvykdymo, dėl, kaip konstatuota pirmiau, savo didelio neatsargumo, atliko tam tikrus veiksmus, kuriuos šalys iš anksto buvo sutarusios įprastomis sąlygomis laikyti pareiškėjos sutikimu vykdyti kortele inicijuotas mokėjimo operacijas. Pagal Lietuvos Respublikos civilinio kodekso 6.206 straipsnį, viena šalis negali remtis kitos šalies neįvykdymu tiek, kiek sutartis neįvykdyta dėl jos pačios veiksmų ar neveikimo arba kitokio įvykio, kurio rizika jai pačiai ir tenka. Nagrinėjamu atveju, Lietuvos banko nuomone, pareiškėja, atlikdama veiksmus, kurie šalių sutartiniuose santykiuose laikomi, jos sutikimu vykdyti mokėjimo operacijas davimu, negalėtų remtis tuo, kad bankas, nežinodamas pirmiau nurodytų aplinkybių, neatsisakė vykdyti jam pateiktų mokėjimų nurodymų atlikti ginčijamas mokėjimo operacijas ir juos šalių iš anksto sutarta tvarka ir sąlygomis priėmė vykdyti, nes būtent pareiškėja, būdama itin neatsargi, pirmoji pažeidė šalių sutartas kortelės ir jos duomenų naudojimo ir saugojimo sąlygas, taip sudarydama galimybę tretiesiems asmenims tariamai pareiškėjos vardu pateikti bankui šiuos mokėjimo nurodymus.

Mokėjimų įstatymo 29 straipsnio 3 dalyje nustatyta, kad mokėtojas bet kuriuo metu iki šio įstatymo 44 straipsnyje nustatyto neatšaukiamumo momento gali panaikinti sutikimą įvykdyti mokėjimo operaciją ir (arba) kelias mokėjimo operacijas. 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. Mokėjimų įstatymo 44 straipsnio 2 dalyje nustatyta, kad kai mokėjimo operacija inicijuojama gavėjo arba per gavėją, mokėtojas negali atšaukti mokėjimo nurodymo po to, kai gavėjui davė sutikimą atlikti mokėjimo operaciją. Kaip matyti, Mokėjimų įstatymo 44 straipsnio 2 dalis nustato ankstesnį, negu to paties straipsnio 1 dalyje nurodytas, mokėjimo nurodymo neatšaukiamumo momentą. Kaip nurodyta pirmiau, tuo metu, kai pareiškėja pranešė bankui apie ginčijamas mokėjimo operacijas, bankas jau buvo gavęs mokėjimo nurodymus vykdyti ginčijamas mokėjimo operacijas, t. y. pareiškėja pateikė bankui Mokėjimų įstatymo 34 straipsnio 1 dalies 2 punkte nurodytą pranešimą po to, kai suėjo Mokėjimų įstatymo 44 straipsnio 1 dalyje ir 2 dalyje nustatyti terminai, per kuriuos mokėtojas turi teisę atšaukti mokėjimo nurodymą. Suėjus šiems terminams, mokėjimo nurodymas gali būti atšauktas tik tada, kai dėl to susitaria mokėjimo paslaugų vartotojas ir atitinkamas mokėjimo paslaugų teikėjas ir yra gaunamas gavėjo sutikimas (Mokėjimų įstatymo 44 straipsnio 4 dalis).

Ginčo byloje nustatytos faktinės aplinkybės, šalių pateikti paaiškinimai ir įrodymai leidžia daryti išvadą, kad pareiškėja galėjo iš anksto, t. y. iki bankas gavo mokėjimo nurodymus vykdyti ginčijamas mokėjimo operacijas ir jų pagrindu rezervavo lėšas pareiškėjos sąskaitoje, pastebėti galimą kortelės duomenų praradimą, neautorizuotą jų naudojimą ir (arba) ketinimą juos naudoti. Kadangi pareiškėja dėl galimo kortelės duomenų praradimo į banką kreipėsi po to, kai šių duomenų pagrindu buvo atliktos ginčijamos mokėjimo operacijos ir bankui buvo pateikti mokėjimo nurodymai jas vykdyti, o bankas, nesant gavėjo sutikimo, nebegalėjo jų atšaukti, darytina išvada, kad nėra pagrindo pareiškėjos atžvilgiu taikyti Mokėjimo įstatymo 39 straipsnio 5 dalies nuostatas.

Byloje nėra duomenų, kad gavėjas būtų davęs sutikimą atšaukti ginčijamos mokėjimo operacijos vykdymą, priešingai – iš bylos duomenų matyti, kad po mokėjimo nurodymų bankui pateikimo, gavėjas (per savo finansų įstaigą) pateikė bankui galutinius patvirtinimus dėl atsiskaitymo kortele, kurių pagrindu bankas nurašė lėšas iš pareiškėjos sąskaitos. Taigi, Mokėjimų įstatymo 44 straipsnio 4 dalyje nurodyta sąlyga (gavėjo sutikimas atšaukti mokėjimo nurodymus) nebuvo tenkinta, todėl ginčijamos mokėjimo operacijos atšaukimas nebuvo galimas.

Įvertinęs pirmiau nurodytas aplinkybes, šalių pateiktus įrodymus ir jų pagrindu padarytas išvadas, Lietuvos bankas mano, kad pareiškėjos elgesys, kuris pasireiškė tuo, kad pareiškėja, gavusi elektroninį laišką su nuoroda, ją atsidariusi atskleidė ne tik savo kortelės duomenis, bet ir vienkartinį saugos kodą, skirtą kortelės pridėjimui prie Apple Pay sistemos patvirtinti, nors, remiantis iš byloje turimų duomenų tokio tikslo galimai neturėjo (pareiškėja teigė, kad norėjo atlikti 5 RON mokėjimą pašto paslaugų teikėjui), taip sudarydama tretiesiems asmenims sąlygas, panaudojant kortelės duomenis ir gautą vienkartinį saugos kodą, pridėti pareiškėjos kortelę prie *Apple Pay* sistemos ir per šią sistemą inicijuoti ginčijamas mokėjimo operacijas iš jos sąskaitos, pripažintinas kaip elgesys, iš esmės besiskiriantis nuo atsargaus elgesio reikalavimų, t. y. laikytinas itin neatsargiu, kuris galiausiai lėmė, kad pareiškėjos sąskaitoje buvo įvykdytos

neautorizuotos ginčijamos mokėjimo operacijos. Byloje turimi duomenys leidžia teigti, kad jeigu nagrinėjamu atveju pareiškėja būtų buvusi pakankamai atidi ir kritiška jai teiktos, anksčiau jau turėtos ir (arba) žinomos informacijos bei savo atliekamų veiksmų atžvilgiu, ji būtų pastebėjusi ir supratusi, kad atlieka veiksmus, kurių, ne tik kad nereikia atlikti, bet ir, laikantis Mokėjimų įstatymo 34 straipsnyje ir Sutarties 9 punkte pareiškėjui nustatytų pareigų, negalima atlikti, ir ginčijamos mokėjimo operacijos galimai nebūtų įvykdytos. Atsižvelgiant į tai, konstatuotina, kad nagrinėjamu atveju yra pagrindas pareiškėjui taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį.

Konstatavus, kad nagrinėjamu atveju yra pagrindas pareiškėjos atžvilgiu taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, nustatančią, kad mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai, ir nenustačius kitų aplinkybių, dėl kurių bankui kiltų (galėtų kilti) pareiga grąžinti pareiškėjai ginčijamų mokėjimo operacijų sumas, pareiškėjos reikalavimas rekomenduoti bankui grąžinti (kompensuoti) pareiškėjai ginčijamų mokėjimo operacijų sumas yra 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 tapataus ginčo dalyko kreiptis į teismą arba kitą ginčų nagrinėjimo instituciją įstatymų nustatyta tvarka. Kreipimasis į teismą po Lietuvos banko sprendimo dėl ginčo esmės priėmimo nelaikomas šio Lietuvos banko 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