LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

SPRENDIMAS DĖL X. X. IR *REVOLUT PAYMENTS UAB* GINČO NAGRINĖJIMO

2022-05-06 Nr. 429-165
Vilnius

Lietuvos bankas gavo pareiškėjo X. X. (toliau – pareiškėjas) kreipimąsi, kuriuo prašoma išnagrinėti tarp pareiškėjo ir *Revolut Payments UAB* (toliau – bendrovė) kilusį ginčą.

N u s t a t y t a:

2020 m. vasario 1 d. pareiškėjas ir bendrovė sudarė mokėjimo paslaugų teikimo sutartį (toliau – Sutartis), kurios pagrindu pareiškėjui buvo atidaryta mokėjimo sąskaita Nr. *(duomenys neskelbtini)* (toliau – sąskaita) ir išduota su šia sąskaita susieta „Visa" mokėjimo kortelė Nr. *(duomenys neskelbtini)* (toliau – kortelė).

2021 m. gruodžio 9 d. kortele per mobiliųjų mokėjimų sistemą „Apple Pay" (toliau – „Apple Pay") buvo atliktos septynios mokėjimo operacijos, kurioms įvykdyti iš pareiškėjo sąskaitos buvo nurašyta bendra 228 214 Japonijos jenų suma (iš viso 5 mokėjimo operacijos) ir bendra 296,07 euro suma (iš viso 2 mokėjimo operacijos) (toliau – ginčijamos mokėjimo operacijos). Nurašytos sumos buvo konvertuotos į Kazachstano tenges ir pervestos prekybininkui „Chuantai", veikiančiam Kazachstano Respublikoje (toliau – lėšų gavėjas).

Pastebėjęs mokėjimo sąskaitoje atliktas ginčijamas mokėjimo operacijas, pareiškėjas tą pačią dieną, t. y. 2021 m. gruodžio 9 d., kreipėsi į bendrovę, informuodamas ją, kad jo atžvilgiu buvo atlikti sukčiavimo veiksmai ir ginčijamas mokėjimo operacijas atliko ne jis. Bendrovės prašymu pareiškėjas tą pačią dieną užpildė prašymą atšaukti šias mokėjimo operacijas. Prašyme paaiškino, kad, bandant per platformą „BlaBlacar" užsakyti pavėžėjimo paslaugą Prancūzijos Respublikoje, su juo per programėlę „WhatsApp" susisiekė nepažįstamas asmuo, prisistatęs šios paslaugos teikėju. Asmuo atsiuntė pareiškėjui nuorodą, kurioje pareiškėjas suvedė savo kortelės duomenis, o vėliau pastebėjo, kad šie duomenys buvo panaudoti ginčijamoms mokėjimo operacijos atlikti. Pareiškėjas pripažino, kad bendraudamas su minėtu asmeniu nebuvo pakankamai atsargus ir perdavė jam savo kortelės duomenis.

Gavusi šią informaciją, bendrovė tą pačią dieną užblokavo pareiškėjo kortelę ir apie tai informavo pareiškėją. Įvertinusi pareiškėjo pateiktą informaciją ir turimus vidaus sistemų duomenis, bendrovė 2021 m. gruodžio 11 d. pranešė pareiškėjui, kad ginčijamos mokėjimo operacijos nebus atšauktos ir jų sumos pareiškėjui nebus grąžintos.

2021 m. gruodžio 11 d. pareiškėjas pakartotinai kreipėsi į bendrovę, prašydamas atšaukti ginčijamas mokėjimo operacijas, o jei tokios galimybės nėra, informuoti jį apie veiksmus, kuriuos jis galėtų (turėtų) atlikti, kad atgautų šių mokėjimo operacijų sumas.

2021 m. gruodžio 23 d. bendrovė informavo pareiškėją, kad savo sprendimo nekeis, ir papildomai paaiškino, kad ginčijamos mokėjimo operacijos netenkina tarptautinės kortelių asociacijos „Visa" (toliau – „Visa") nustatytų mokėjimo kortele atliktų mokėjimo operacijų atšaukimo sąlygų, todėl bendrovė negali inicijuoti jų atšaukimo.

2022 m. sausio 10 d. pareiškėjas kreipėsi į Lietuvos banką, prašydamas išspręsti tarp šalių kilusį ginčą ir rekomenduoti bendrovei grąžinti jam ginčijamų mokėjimo operacijų sumas. Kreipimesi nurodo, kad ginčijamos mokėjimo operacijos buvo atliktos apgaulės būdu, t. y. trečiajam asmeniui išviliojant iš pareiškėjo jo kortelės duomenis ir panaudojant juos ginčijamoms mokėjimo operacijoms atlikti. Jokių ryšių su Kazachstano Respublika, kurioje įsteigtas lėšų gavėjas, pareiškėjas teigia neturintis. Papildomai nurodo, kad dėl trečiojo asmens neteisėtų veiksmų 2021 m. gruodžio 29 d. kreipėsi į gyvenamosios vietos policijos įstaigą.

Atsiliepime į pareiškėjo kreipimąsi bendrovė nurodo nesutinkanti su pareiškėjo

reikalavimu ir prašo jį atmesti. Bendrovės teigimu, atsakomybė už ginčijamų mokėjimo operacijų atlikimą tenka pačiam pareiškėjui. Bendrovės vidaus sistemų duomenimis, ginčijamos mokėjimo operacijos buvo tinkamai autorizuotos, jų inicijavimo ir vykdymo metu nebuvo užfiksuota jokių techninių ar kitokių trikdžių, kurie galėjo jas kaip nors paveikti. Pareiškėjo paskyros mobilioje programėlėje „Revolut" ir kortelės pasisavinimo požymių bei bandymų jungtis prie pareiškėjo sąskaitos iš kito, negu pareiškėjas įprastai naudoja, įrenginio taip pat nebuvo nustatyta. Nors bendrovė laiko pareiškėjo ginčijamas mokėjimo operacijas jo paties autorizuotomis, papildomai atkreipia dėmesį, kad, bendrovės nuomone, aptariamoje situacijoje pareiškėjas elgėsi itin neatsargiai, nesilaikė bendrovės ir pareiškėjo sutartų kortelės ir jos duomenų naudojimo bei saugojimo sąlygų ir taip sudarė sąlygas ginčijamoms mokėjimo operacijoms įvykti.

Bendrovė pateikė vidaus sistemų duomenis, liudijančius, kad iki ginčijamų mokėjimo operacijų inicijavimo ir atlikimo pareiškėjo kortelė buvo pridėta prie „Apple Pay" ir šios mokėjimo operacijos buvo atliktos būtent per šią sistemą. Bendrovė paaiškino, kad, norint mokėjimo kortele atlikti mokėjimus per „Apple Pay", vien tik nurodyti (atskleisti) mokėjimo kortelės duomenis nepakanka, nes mokėjimo kortelės pridėjimą būtina patvirtinti vienkartiniu saugos kodu, kuris siunčiamas SMS žinute į mokėjimo kortelės turėtojo mobilųjį telefoną. Bendrovės teigimu, tokia žinutė yra siunčiama tik į tą mobiliojo telefono numerį, kurį mokėjimo paslaugų sutarties sudarymo metu bendrovei nurodo ir patvirtina patys klientai. Tokią SMS žinutę, kaip nurodo bendrovė, į savo mobilųjį telefoną turėjo gauti ir pareiškėjas. Mobiliojo telefono, kuriuo įprastai naudojasi, pareiškėjas nebuvo praradęs, todėl, bendrovės įsitikinimu, joks kitas asmuo, išskyrus pareiškėją, negalėjo gauti asmeniškai į pareiškėjo mobilųjį telefoną atsiųsto saugos kodo. Jei saugos kodas tapo žinomas tretiesiems asmenims, tai tik dėl to, kad pareiškėjas aktyviais veiksmais jį perdavė (atskleidė) šiems asmenims.

Bendrovė papildomai atkreipė dėmesį, kad Lietuvos Respublikos mokėjimų įstatymo 34 straipsnyje nustatyta mokėtojo (nagrinėjamu atveju – pareiškėjo) pareiga, gavus mokėjimo priemonę, imtis veiksmų, kad būtų apsaugoti personalizuoti saugumo duomenys, o sužinojus apie mokėjimo priemonės praradimą, vagystę arba neteisėtą pasisavinimą ar neautorizuotą jos naudojimą, nedelsiant apie tai pranešti mokėjimo paslaugų teikėjui arba jo nurodytam subjektui, taip pat nurodė, kad analogiškos pareigos nustatytos ir bendrovės ir pareiškėjo sudarytos Sutarties 9 dalyje: *„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. <...>"*

Komentuodama atsisakymo inicijuoti mokėjimų atšaukimo procedūrą priežastis, bendrovė nurodo, kad, vadovaujantis „Visa" pagrindinių taisyklių ir „Visa" produktų ir paslaugų taisyklių (angl. *Visa Core Rules and Visa Product and Servise Rules)* (toliau – „Visa" taisyklės) 11 skyriaus 7 punktu „Ginčo kategorija: sukčiavimas", mokėjimo kortele atliktos mokėjimo operacijos atšaukimas tuo pagrindu, kad ji atlikta sukčiaujant, yra negalimas, kai mokėjimo kortelės turėtojas dalyvauja ją atliekant ir (arba) duoda savo sutikimą ją atlikti. Įvertinusi tai, kad pareiškėjas pats perdavė savo kortelės duomenis trečiajam asmeniui, pats susiejo ir (arba) sudarė sąlygas susieti kortelę su „Apple Pay", kurią naudojant buvo atliktos ginčijamos mokėjimo operacijos, ir tokį susiejimą papildomai pats patvirtino ir (arba) sudarė sąlygas patvirtinti asmeniškai gautu vienkartiniu saugos kodu, taip duodamas sutikimą vykdyti kortele inicijuotas mokėjimo operacijas, bendrovė konstatavo, kad ginčijamoms mokėjimo operacijoms taikomi „Visa" taisyklių 11 skyriaus 7 punkte „Ginčo kategorija: sukčiavimas" nustatyti ribojimai, dėl kurių šių operacijų atšaukimas ir jų sumų grąžinimas pareiškėjui nebuvo galimas. Bendrovės teigimu, užginčyti ir atšaukti ginčijamas mokėjimo operacijas nebuvo galimybės ir dėl to, kad jos atliktos naudojant bekontaktį atsiskaitymo metodą (per „Apple Pay"), kuriam, remiantis Visa taisyklių 11 skyriaus 7 punkto 3.3 papunkčiu, atšaukimo procedūra iš viso netaikoma.

Paprašytas pakomentuoti kortelės pridėjimo prie „Apple Pay" bei ginčijamų mokėjimo operacijų atlikimo per šią sistemą aplinkybes, pareiškėjas nurodė nežinojęs, kad ginčijamos mokėjimo operacijos buvo atliktos per „Apple Pay". Pareiškėjas teigia naudojantis mobilųjį telefoną su „Android" operacine sistema ir iki ginčijamų mokėjimo operacijų atlikimo nebuvo pridėjęs jokių savo turimų mokėjimo kortelių prie „Apple Pay", taip pat neatliko jokių veiksmų, kuriais būtų patvirtinęs kortelės pridėjimą prie „Apple Pay", davęs savo sutikimą ją pridėti ir

(arba) atlikti ginčijamas mokėjimo operacijas per šią sistemą. Pareiškėjas taip pat neigia gavęs į savo mobiliųjų telefoną SMS žinutę su vienkartiniu saugos kodu. Pareiškėjo įsitikinimu, trečiajam asmeniui pridedant pareiškėjo kortelę prie „Apple Pay", bendrovė galimai neprašė patvirtinti tokio kortelės pridėjimo jokiais saugos kodais ar kitokiais slaptažodžiais ir taip sudarė galimybę trečiajam asmeniui pridėti šią kortelę prie „Apple Pay" ir per šią sistemą atlikti ginčijamas mokėjimo operacijas be pareiškėjo žinios ir sutikimo.

Bendrovė taip pat patvirtino, kad, jos turimais duomenimis, pareiškėjas naudoja mobilųjį telefoną su „Android" operacine sistema, o jo kortelė prie „Apple Pay" buvo pridėta naudojant visai kitą įrenginį. Nepaisant to, bendrovės įsitikinimu, vienkartinis saugos kodas, skirtas kortelės pridėjimui prie „Apple Pay" patvirtinti, turėjo būti išsiųstas būtent į pareiškėjo mobilųjį telefoną, nes kitu atveju kortelės pridėjimas prie „Apple Pay" nebūtų buvęs galimas, tačiau tai patvirtinančių įrodymų nepateikė. Atsižvelgdama į tai, kad pareiškėjo žinioje buvusi kortelė buvo pridėta prie „Apple Pay", bendrovė daro išvadą, kad pareiškėjas aktyviais veiksmais leido pridėti jo kortelę prie „Apple Pay", o tokių veiksmų atlikimas, kaip teigia bendrovė, remiantis šalių sudarytos Sutarties 14 punktu, reiškia pareiškėjo sutikimą vykdyti per „Apple Pay" inicijuotas mokėjimo operacijas (nagrinėjamu atveju – ginčijamas mokėjimo operacijas).

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. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą ir jo pagrindu priimamas sprendimas.

Atsižvelgiant į ginčo šalių pateiktus paaiškinimus ir įrodymus, darytina išvada, kad šalių ginčas kilo dėl bendrovės atsisakymo grąžinti pareiškėjui ginčijamų mokėjimo operacijų sumas. Pareiškėjo vertinimu, bendra atliktų ginčijamų mokėjimo operacijų vertė eurais siekia 2 060 eurų. Remiantis bendrovės pateikta informacija apie ginčijamų mokėjimo operacijų atlikimo metu galiojusį Japonijos jenos ir euro kursą, bendra ginčijamų mokėjimo operacijų vertė eurais sudarė 2 076,39 euro.

Pareiškėjas teigia, kad ginčijamos mokėjimo operacijos buvo įvykdytos be jo sutikimo, trečiajam asmeniui apgaulės būdu išviliojus iš pareiškėjo kortelės duomenis, kurie be jo žinios ir sutikimo vėliau buvo panaudoti kortelės pridėjimui prie „Apple Pay" tvirtinti ir ginčijamoms mokėjimo operacijoms atlikti per šią sistemą, todėl bendrovė turi grąžinti pareiškėjui ginčijamų mokėjimo operacijų sumas. Bendrovė teigia, kad ginčijamos mokėjimo operacijos buvo autorizuotos šalių sudarytoje Sutartyje nustatytu būdu, atliktos per „Apple Pay", prie kurios naudojantis tik pareiškėjui žinomu vienkartiniu saugos kodu buvo pridėta ir patvirtina pareiškėjo kortelė, todėl bendrovė neturi pareigos grąžinti pareiškėjui ginčijamų mokėjimo operacijų sumų.

Siekiant išspręsti tarp pareiškėjo ir bendrovės kilusį ginčą, Lietuvos banko vertinimu, būtina nustatyti, ar ginčijamos mokėjimo operacijos laikytinos autorizuotomis ir ar bendrovė turėjo (turi) pareigą grąžinti pareiškėjui ginčijamų mokėjimo operacijų sumas.

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.

Mokėjimų įstatymo 29 straipsnio 1 dalyje nustatyta, kad mokėjimo operacija laikoma autorizuota tik tada, kai mokėtojas duoda sutikimą ją vykdyti (toliau – sutikimas). 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 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 arba 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).

Pažymėtina, kad Mokėjimų įstatymas neapibrėžia konkrečių sutikimo formai, turiniui ar jo davimo būdui taikomų reikalavimų. 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.

Pareiškėjo ir bendrovės sudarytos Sutarties 14 punkte „Kitų tipų mokėjimai“ nustatyta, kad *„Sutikimą atlikti mokėjimus savo „Revolut“ kortele taip pat duodate*: <..> *pateikdami „Revolut“ kortelės numerį ir kitą informaciją ir sutikdami inicijuoti mokėjimo nurodymus dėl jūsų sąskaitos nurašymo sudarant sutartį su prekybininku ar paslaugų teikėju; arba pateikdami „Revolut“ kortelės numerį ir kitą informaciją prekybininkui ar paslaugų teikėjui ir patvirtindami šį mokėjimą naudojant „3D Secure“ metodą. Tai yra žingsnis, kurį turėsite atlikti atsiskaitydami internetu naudojant „Revolut“ kortelę, jei prekybininkas ar paslaugų teikėjas įdiegė šį metodą. Jei jie įdiegė šį metodą, prekybininko ar paslaugų teikėjo internetinėje svetainėje pasirodys langas, kuriame prašoma patvirtinti mokėjimą, o jūs gausite iššokantį pranešimą į „Revolut“ programėlę. Norėdami užbaigti mokėjimą, turėsite atidaryti programėlę ir patvirtinti operaciją.*“

Bendrovės teigimu, perduodamas trečiajai šaliai savo kortelės duomenis bei leisdamas patvirtinti šios kortelės pridėjimą prie „Apple Pay“ tik jam žinomu vienkartiniu saugos kodu, kuris buvo atsiųstas į jo mobilųjį telefoną, pareiškėjas atliko Sutarties 14 punkte nurodytus veiksmus, kurie šalių santykiuose laikomi sutikimo vykdyti mokėjimo kortele grindžiamas mokėjimo operacijas davimu. Remiantis bendrovės pateiktais paaiškinimais bei Sutarties 14 punkte nurodytomis sutikimo vykdyti mokėjimo kortele inicijuotas mokėjimo operacijas davimo sąlygomis, darytina išvada, kad bendrovė ir pareiškėjas buvo sutarę, kad mokėjimo kortele grindžiamų mokėjimo operacijų atlikimo per „Apple Pay“ atveju pareiškėjo sutikimas vykdyti per šią sistemą atliktas mokėjimo operacijas yra duodamas pridėjus kortelę prie „Apple Pay“ ir patvirtinus tokį kortelės pridėjimą tam skirtu vienkartiniu saugos kodu (saugesnis autentiškumo patvirtinimo būdas), o tokiu būdu duotas sutikimas yra daugkartinio pobūdžio, t. y. duodamas visoms paskesnėms per „Apple Pay“ atliekamoms mokėjimo operacijoms įvykdyti.

Savo interneto svetainėje bendrovė yra nurodžiusi, kad *„Turimas „Revolut“ korteles gali pridėti prie šių įrenginių: iPhone SE“ ar naujesnių modelių; „iPad 3“ ar naujesnių modelių; visų „Apple Watch“ modelių; „Mac“ modelių su „Touch ID“* (https://www.revolut.com/lt-LT/help/making-payments/spending/paying-with-apple-or-google-pay/am-i-eligible-for-apple-pay) bei *„Kad pridėtum savo kortelę prie „Apple Pay“: Eik į skirtuką „Kortelės“, kad galėtum pasirinkti norimą kortelę. Spustelk mygtuką „Pridėti prie „Apple Wallet“. Taip pat gali suvesti savo „Revolut“ kortelės duomenis tiesiai „Apple Pay“ programėlėje.“ (https://www.revolut.com/lt-LT/help/making-payments/spending/paying-with-apple-or-*

google-pay/setting-up-apple-pay).

Remiantis šalių pateiktais paaiškinimais, darytina išvada, kad tarp šalių nėra ginčo dėl to, kad jas siejančių sutartinių santykių metu pareiškėjas naudojo turimą mobilųjį telefoną, kuriame įdiegta „Android" operacinė sistema, nesudaranti galimybės šiuo telefonu naudotis „Apple Pay", todėl pareiškėjo kortelė buvo pridėta prie „Apple Pay" naudojant kitą įrenginį. Kaip minėta pirmiau, pareiškėjas neneigia trečiajam asmeniui atskleidęs savo kortelės duomenis, tačiau neigia naudojęs „Apple Pay", pridėjęs prie jos savo kortelę ar davęs sutikimą trečiajam asmeniui ją pridėti, taip pat neigia gavęs ir (ar) perdavęs trečiajam asmeniui kortelės pridėjimui patvirtinti skirtą saugos kodą, kurį, bendrovės teigimu, turėjo gauti į savo mobilųjį telefoną, ir (ar) atlikęs kitokio pobūdžio patvirtinimo veiksmus. Atsižvelgdamas į tai, kad Lietuvos bankas neturi galimybės nustatyti, ar įrenginys, kuriuo pareiškėjo kortelė buvo pridėta prie „Apple Pay", priklauso pareiškėjui, bei į tai, kad pareiškėjas ne tik tai neigia, bet ir teigia nežinojęs apie tokį kortelės pridėjimą, o bendrovė nepateikė jokių įrodymų, kurie patvirtintų priešingai, Lietuvos bankas daro išvadą, kad nagrinėjamu atveju labiau tikėtina, jog pareiškėjo kortelę prie „Apple Pay" savo valdomame įrenginyje pridėjo trečiasis asmuo, kuriam pareiškėjas perdavė savo kortelės duomenis. Taigi, nepaisant to, kad pareiškėjas perdavė trečiajam asmeniui kortelės duomenis, labiau tikėtina, kad šiuos duomenis paskesniam jų gavėjui (nagrinėjamu atveju – „Apple Pay") perdavė ne pats pareiškėjas.

Vertinant bendrovės nurodytas prielaidas, kad pareiškėjas galėjo perduoti kortelės pridėjimui prie „Apple Pay" skirtą vienkartinį saugos kodą, gautą į savo mobilųjį telefoną, Lietuvos banko nuomone, būtina atsižvelgti į tai, kad bendrovė nepateikė jokių įrodymų, pagrindžiančių, kad, priešingai, nei teigia pareiškėjas, šis kodas buvo išsiųstas pareiškėjui. Lietuvos bankas neturi galimybės patikrinti, kurios iš šalių pateikta informacija yra teisinga, t. y. ar pareiškėjas, kaip teigia bendrovė, buvo gavęs į jo mobilųjį telefoną siųstą saugos kodą ir perdavęs jį trečiajam asmeniui, ar, kaip teigia pareiškėjas, bendrovė pareiškėjui nebuvo siuntusi tokio kodo ir jis atitinkamai negalėjo perduoti ir neperdavė jo trečiajam asmeniui, kuris, panaudodamas šį kodą, pridėjo pareiškėjo kortelę prie „Apple Pay" ir vėliau šioje sistemoje atliko ginčijamas mokėjimo operacijas, tačiau, vadovaudamasis Mokėjimų įstatymo 37 straipsnio 1 dalimi, įtvirtinančia bendrovės pareigą įrodyti ginčijamų mokėjimo operacijų autentiškumo patvirtinimą, ir atsižvelgdamas į tai, kad bendrovė nepateikė jokių įrodymų, pagrindžiančių, kad bendrovė buvo siuntusi pareiškėjui kortelės pridėjimui prie „Apple Pay" patvirtinti skirtą vienkartinio saugumo kodą, daro išvadą, kad nagrinėjamu atveju bendrovė neįrodė, kad ginčijamų mokėjimo operacijų autentiškumas (sudėtinė sutikimo vykdyti mokėjimo kortele grindžiamas mokėjimo operacijos davimo dalis) buvo tinkamai patvirtintas ir ginčijamos mokėjimo operacijos buvo atliktos esant pareiškėjo sutikimui, kaip jis suprantamas Mokėjimų įstatymo 29 straipsnio 1 dalyje ir Sutarties 14 punkte.

Svarbu pažymėti, kad Mokėjimų įstatymo 58 straipsnio 1 dalis įpareigoja bendrovę taikyti saugesnio autentiškumo patvirtinimo procedūrą, kai mokėtojas (nagrinėjamu atveju – pareiškėjas): 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. Remiantis bendrovės pateikta informacija, nagrinėjamo ginčo atveju tokia procedūra laikytina mokėjimo kortelės pridėjimo prie „Apple Pay" patvirtinimo personalizuotu vienkartiniu saugos kodu, kuris siunčiamas į mokėjimo kortelės turėtojo mobilųjį telefoną, panaudojimu. Kaip minėta pirmiau, bendrovė nepateikė įrodymų, patvirtinančių SMS žinutės su vienkartiniu saugos kodu išsiuntimą pareiškėjui, taip pat nepateikė kitų įrodymų, kurie leistų teigti, kad pareiškėjas buvo gavęs tokią SMS žinutę, įvedęs tokį saugos kodą ir (ar) perdavęs jį trečiajam asmeniui, kuris panaudojo jį kortelės pridėjimui prie „Apple Pay" patvirtinti, o vėliau ginčijamoms mokėjimo operacijoms atlikti.

Įvertinęs šalių pateiktus duomenis apie ginčijamų mokėjimo operacijų atlikimo aplinkybes, pakankamo pagrindo pripažinti ginčijamas mokėjimo operacijas autorizuotomis, t. y. atliktomis esant pareiškėjo sutikimui, kaip jis suprantamas Mokėjimų įstatymo 29 straipsnio 1 dalies kontekste ir Sutarties 14 punkte, Lietuvos bankas nenustatė, todėl daro išvadą, kad ginčijamos mokėjimo operacijos laikytinos neautorizuotomis, kaip tai nurodyta Mokėjimų įstatymo 29 straipsnio 2 dalyje.

Bendrovės vertinimu, pareiškėjo veiksmai, kuriais jis perdavė nežinomam asmeniui savo kortelės duomenis ir, kaip teigia bendrovė, vienkartinį saugos kodą, kuriuo buvo patvirtintas kortelės pridėjimas prie „Apple Pay", turi didelio neatsargumo požymių, kurie pasireiškia Mokėjimų įstatymo 34 straipsnyje pareiškėjui, kaip teisėtam kortelės naudotojui, nustatytų

pareigų, susijusių su jam išduotos kortelės ir jos personalizuotų saugumo duomenų (įskaitant vienkartinį saugos kodą, skirtą kortelės pridėjimui prie „Apple Pay" patvirtinti) saugojimu, nesilaikymu, taip pat Sutartyje įtvirtintų analogiškų įsipareigojimų nevykdymu. Vadovaujantis Mokėjimų įstatymo 39 straipsnio 4 dalimi, kai mokėtojo mokėjimo paslaugų teikėjas nereikalauja saugesnio autentiškumo patvirtinimo, mokėtojui dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai tenka tik tuo atveju, jeigu jis veikė nesąžiningai. Duomenų, kurie leistų vertinti pareiškėjo veiksmus kaip nesąžiningus, nebuvo nustatyta. Tokio pobūdžio klausimų nekelia ir pati bendrovė. Kaip minėta pirmiau, bendrovė nepateikė įrodymų, patvirtinančių, kad šio ginčo byloje ji įgyvendino Mokėjimų įstatymo 58 straipsnio 1 dalyje jai nustatytus reikalavimus, t. y. nepateikė įrodymų, patvirtinančių, kad taikė saugesnio autentiškumo patvirtinimo procedūrą ir buvo išsiuntusi į pareiškėjo mobilųjį telefoną vienkartinį saugos kodą, skirtą kortelės pridėjimui prie „Apple Pay" patvirtinti. Atsižvelgdamas į tai, Lietuvos bankas daro išvadą, kad bendrovė neįrodė, kad vykdydama ginčijamas mokėjimo operacijas laikėsi Mokėjimų įstatyme įtvirtintų saugesnio autentiškumo patvirtinimo reikalavimų. Taigi, Lietuvos banko nuomone, bendrovei gali būti taikytinos Mokėjimų įstatymo 38 straipsnio 1 dalies bei 39 straipsnio 4 dalies nuostatos, nustatančios bendrovės pareigą grąžinti pareiškėjui neautorizuotų mokėjimo operacijų sumas, t. y. ginčijamų mokėjimo operacijų sumas.

Atsižvelgdamas į pareiškėjo ir bendrovės įvardytų ginčijamų mokėjimo operacijų verčių eurais skirtumus, Lietuvos bankas mano, kad turėtų būti vadovaujamasi bendrovės nurodyta ginčijamų mokėjimo operacijų sumos eurais verte (2 076,39 euro), nes ji, kaip nurodė pati bendrovė, yra apskaičiuota, remiantis atliekant ginčijamas mokėjimo operacijas taikytu Japonijos jenų ir euro kursu.

Remdamasis tuo, kas išdėstyta, ir vadovaudamasis 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:

1. Tenkinti pareiškėjo X. X. reikalavimą ir rekomenduoti *Revolut Payments UAB* grąžinti (kompensuoti) pareiškėjui 2 076,39 euro sumą.
2. Įpareigoti *Revolut Payments UAB* per mėnesį nuo šio sprendimo priėmimo dienos raštu informuoti Lietuvos banką apie šio sprendimo rezoliucinės dalies 1-ame punkte nurodytos rekomendacijos įgyvendinimą (neįgyvendinimą). Bendrovei neįvykdžius minėtos rekomendacijos, apie tai bus paskelbta Lietuvos Respublikos teisės aktų nustatyta tvarka.

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