# LIETUVOS BANKO FINANSŲ RINKŲ PRIEŽIŪROS TARNYBOS TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

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

2021-09-16 Nr. 429-338
Vilnius

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

Nustatyta:

2021 m. balandžio 15 d. pareiškėjui bendrovės išduota mokėjimo kortele panaudojant *Apple Pay* mokėjimo nurodymo patvirtinimo metodą buvo atliktos dvi mokėjimo operacijos: 23:31:46 val. 100 Eur mokėjimo operacija gavėjai *Pizzeria Tuyas* bei 23:33:18 val. 100 Eur mokėjimo operacija gavėjai *Pizzeria Tuyas* (toliau – ginčijamos mokėjimo operacijos).

2021 m. balandžio 16 d. pareiškėjas kreipėsi į bendrovę ir nurodė, kad jam priklausančia mokėjimo kortele buvo neteisėtai atsiskaityta. Pareiškėjas užpildė prašymą grąžinti, pareiškėjo teigimu, jo neautorizuotų mokėjimo operacijų lėšas. Pareiškėjas bendrovei nurodė, kad mokėjimo kortelės nebuvo praradęs ir niekam jos nebuvo perdavęs, ji visą laiką buvo su pareiškėju jo namuose Maltoje, o ginčijamos mokėjimo operacijos atliktos Ispanijoje.

Bendrovė atlikusi tyrimą 2021 m. gegužės 6 d. priėmė sprendimą atsisakyti pareiškėjui grąžinti jo ginčijamų mokėjimo operacijų sumą, nes bendrovė nerado jokių apgaulingos veiklos požymių, dėl to, bendrovės nuomone, pats pareiškėjas yra atsakingas už atliktas ginčijamas mokėjimo operacijas.

Pareiškėjas nesutiko su bendrovės sprendimu, todėl kreipėsi į Lietuvos banką dėl vartojimo ginčo nagrinėjimo. Kreipimesi pareiškėjas nurodė, kad bendrovės kortele naudojasi nuo 2018 m. birželio 30 d. Pradėdamas naudotis bendrovės paslaugomis manė, kad bendrovė užtikrina atsiskaitymų saugumą, tačiau 2021 m. balandžio 15 d. pastebėjo, kad jo mokėjimo kortelė buvo pasisavinta ir kad tretieji asmenys be pareiškėjo sutikimo panaudodami pareiškėjo mokėjimo kortelės duomenis įvykdė dvi ginčijamas mokėjimo operacijas. Ginčijamos mokėjimo operacijos buvo įvykdytos Ispanijoje gavėjai *Pizzeria Tuyas*. Pareiškėjas teigia, kad tada, kai buvo atliekamos ginčijamos mokėjimo operacijos, buvęs savo namuose Maltoje ir nesinaudojo bendrovės mokėjimo kortele. Pareiškėjas paaiškino, kad jis neautorizavo ginčijamų mokėjimo operacijų, o sužinojęs apie neteisėtą jo mokėjimo kortelės panaudojimą, užblokavo mokėjimo kortelę ir paprašė bendrovės išduoti naują mokėjimo kortelę. Pareiškėjas paaiškino, kad bendrovė, gavusi pareiškėjo prašymą grąžinti neautorizuotų mokėjimo operacijų lėšas, jas jam grąžino su sąlyga, kad lėšų gavėja sutiks grąžinti pareiškėjo ginčijamų mokėjimo operacijų lėšas. Tačiau 2021 m. gegužės 5 d. bendrovė pakartotinai iš pareiškėjo kortelės sąskaitos nurašė ginčijamų mokėjimo operacijų sumą. Pareiškėjas prašė rekomenduoti bendrovei grąžinti pareiškėjo ginčijamų mokėjimo operacijų sumą – 200 Eur.

Papildomai pareiškėjas informavo, kad nesinaudoja jokiu *Apple* įrenginiu ir kad mokėjimo kortelės prie *Apple Pay* sistemos neregistravo, taip pat teigė, kad iš bendrovės nebuvo gavęs SMS žinutės su vienkartiniu saugos kodu, kuris buvo panaudotas pareiškėjo mokėjimo kortelę priregistruojant prie *Apple Pay* sistemos.

Bendrovė Lietuvos bankui pateiktame atsiliepime nurodė, kad nesutinka tenkinti pareiškėjo reikalavimo. Bendrovė paaiškino, kad išanalizavusi vidinės kontrolės sistemos duomenis nustatė, kad ginčijamos mokėjimo operacijos buvo atliktos panaudojant bekontaktį mokėjimo metodą *Apple Pay*, mokėjimus atliekant fiziniame kasos terminale.

Bendrovės teigimu, pareiškėjas jai nurodęs, jog mokėjimo kortelė, kuria buvo atliktos ginčijamos mokėjimo operacijos, visą laiką buvo pareiškėjo žinioje – ji nebuvo pavogta ir (ar)

pamesta. Bendrovė teigia, kad atlikusi tyrimą neužfiksavo jokių pareiškėjo mokėjimo kortelės perėmimo požymių, neužfiksavo ir duomenų, kad pareiškėjo kortelė galėjo būti pasisavinta trečiųjų asmenų. Pareiškėjas bendrovei taip pat nenurodė, kad buvo pakliuvęs į situaciją, dėl kurios būtų buvęs priverstas atskleisti mokėjimo kortelės duomenis tretiesiems asmenims. Bendrovė pažymėjo, kad, norėdamas pridėti mokėjimo kortelę prie *Apple Pay* sistemos, kuria siekiama atlikti mokėjimo operacijas, mokėjimo kortelės turėtojas turi suvesti mokėjimo kortelės duomenis (mokėjimo kortelės numerį, kortelės saugos kodą (CVV)) ir papildomai patvirtinti mokėjimo kortelės pridėjimą prie *Apple Pay* sistemos įvedant vienkartinį saugos kodą, kurį mokėjimo kortelės savininkas gauna SMS žinute. Minėta žinutė su vienkartiniu saugos kodu visais atvejais yra siunčiama į telefono numerį, kuris buvo nurodytas ir autorizuotas vartotojo sudarant sutartį su bendrove.

Bendrovė paaiškino, kad pareiškėjui žinutę su vienkartiniu saugos kodu siuntė pareiškėjo sutartyje nurodytu telefono numeriu, kurį pareiškėjas buvo patvirtinęs sudarydamas su bendrove mokėjimo paslaugų teikimo sutartį. Bendrovė pabrėžė, kad, jos turimais duomenimis iš sistemų, pareiškėjo mokėjimo kortelė buvo pridėta prie *Apple Pay* sistemos ir buvo įvestas SMS žinute gautas vienkartinis saugos kodas. Bendrovės teigimu, pareiškėjas arba pats mokėjimo kortelę pridėjo prie *Apple Pay* sistemos ir suvedė vienkartinį SMS žinute į jo telefono numerį gautą saugos kodą, arba elgėsi aplaidžiai ir nerūpestingai, nes pateikė (atskleidė) saugos kodą tretiesiems asmenims. Kadangi, bendrovės turimais duomenimis, mokėjimo kortelė buvo pridėta prie *Apple Pay* sistemos ir buvo suvestas vienkartinis SMS žinute į pareiškėjo telefono numerį gautas saugos kodas, bendrovė teigia, kad negali tenkinti pareiškėjo prašymo grąžinti ginčijamas mokėjimo operacijų lėšas.

Bendrovė paaiškino, kad Mokėjimų įstatymo 34 straipsnyje nustatyta mokėtojo 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. Analogiškos pareigos nustatytos ir bendrovės ir pareiškėjo sudarytos paslaugų teikimo 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. <...>"

Bendrovė pabrėžė, kad ginčijamos mokėjimo operacijos buvo atliktos naudojantis *Apple Pay* mokėjimo sistema, prie jos buvo pridėta pareiškėjo mokėjimo kortelė, o operacija patvirtinta įvedant saugos kodą. Atliekant mokėjimą naudojantis *Apple Pay* sistema reikia papildomai patvirtinti mokėjimą, naudojant arba slaptažodį, arba biometrinius duomenis (piršto antspaudą), arba veido atpažinimo technologiją (angl. *Face ID*). Bendrovė paaiškino neturinti duomenų, kokiu būdu pridėjus kortelę prie *Apple Pay* įrenginio buvo patvirtintos ginčijamos mokėjimo operacijos.

Bendrovės teigimu, pareiškėjas patvirtino, kad mokėjimo kortelė buvo jo žinioje. Taigi, net jei kortelės duomenys buvo atskleisti tretiesiems asmenims ar įgyti be mokėjimo kortelės savininko žinios, praktiškai yra neįmanoma, kad trečioji šalis galėjo turėti mokėjimo kortelės duomenis ir gauti saugos kodą, kuris buvo išsiųstas į pareiškėjo telefono numerį. Bendrovės teigimu, atsižvelgiant į tai, kad ginčijamų mokėjimo operacijų autentiškumo patvirtinimo procedūra buvo atlikta tinkamai, tikėtina, kad arba pareiškėjas pats atliko ir patvirtino ginčijamas mokėjimo operacijas suprasdamas savo veiksmus, arba pareiškėjas elgėsi netinkamai ir nerūpestingai, dėl to jo mokėjimo kortelės, kuria buvo atliktos mokėjimo operacijos, duomenys bei trumpoji SMS žinutė buvo atskleisti tretiesiems asmenims.

Atsižvelgdama į pirmiau išdėstytą informaciją, bendrovė teigia, kad nuostolius, susijusius su pareiškėjo ginčijamomis mokėjimo operacijomis, turi prisiimti pats pareiškėjas, o pareiškėjo reikalavimas bendrovei grąžinti pareiškėjo ginčijamų mokėjimo operacijų lėšas yra nepagrįstas.

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.

Pareiškėjo ir bendrovės ginčas kilo dėl bendrovės atsisakymo grąžinti pareiškėjui pareiškėjo mokėjimo kortele panaudojant *Apple Pay* mokėjimo metodą atliktų 200 Eur ginčijamų mokėjimo operacijų, kurioms pareiškėjas teigia nedavęs sutikimo, sumą.

Pareiškėjas teigia nedavęs sutikimo įvykdyti ginčijamas mokėjimo operacijas, o lėšos iš jo mokėjimo kortelės sąskaitos buvo nurašytos dėl to, kad tretieji asmenys pasisavino pareiškėjo mokėjimo kortelės duomenis, todėl bendrovė turi grąžinti pareiškėjui šių mokėjimo operacijų sumą. Bendrovė teigia, kad ginčijamos mokėjimo operacijos buvo įvykdytos panaudojant *Apple Pay* mokėjimo metodą ir fiziškai pridėjus *Apple* įrenginį prie mokėjimo kortelių terminalo. Bendrovės teigimu, jos sistemų duomenys patvirtina, kad pareiškėjo mokėjimo kortelė buvo priregistruota prie *Apple Pay* panaudojant mokėjimo kortelės duomenis (kortelės numerį, CVV kodą) bei kortelės pridėjimą patvirtinant pareiškėjo sutartyje nurodytu telefono numeriu bendrovės išsiųstoje žinutėje pateiktu vienkartiniu saugos kodu. Bendrovės teigimu, mokėjimo operacijas autorizavo arba pats pareiškėjas, arba pareiškėjas dėl didelio neatsargumo atskleidė tretiesiems asmenis mokėjimo kortelės duomenis bei vienkartinį saugos kodą, dėl to tretieji asmenys galėjo įgyti galimybę, pasinaudojant pareiškėjo dėl didelio neatsargumo atskleistais duomenimis, inicijuoti ginčijamas mokėjimo operacijas.

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 sumą.

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 (redakcija, galiojanti nuo 2020 m. spalio 1 d.).

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).

Pažymėtina, kad Mokėjimų įstatyme nėra nustatytų konkrečių mokėtojo sutikimo įvykdyti mokėjimo operaciją būdų ir (arba) detalios tokio sutikimo davimo tvarkos. Vadovaujantis Mokėjimų įstatymo 13 straipsnio 3 dalies 3 punktu ir 29 straipsnio 1 punktu, mokėtojo sutikimo įvykdyti mokėjimo operaciją davimo sąlygos ir tvarka turi būti aptartos mokėtojo ir jo mokėjimo paslaugų teikėjo sudaromoje bendrojoje mokėjimo paslaugų teikimo sutartyje (toliau – bendroji sutartis).

Bendrovės ir pareiškėjo sudarytos sutarties 14 punkte pareiškėjas ir bendrovė buvo sutarę, kad mokėjimai gali būti autorizuojami įvedant mokėjimo kortelės duomenis (kortelės numerį, galiojimo datą, CVV kodą) arba PIN kodą. Šiuos veiksmus bendrovė laiko mokėtojo sutikimu atlikti mokėjimus iš bendrovės sąskaitos (angl. *you can also make payments or withdraw cash using your Revolut Card. You can do this by entering the details of your Revolut Card (the card number, expiry date and CVC number) or your PIN. We will consider these actions as you giving consent to make payments or withdraw cash from your Revolut account*). Bendrosios sutarties 14 punkte nustatyta, kad sutikimą atlikti mokėjimo operacijas kortele taip pat galima duoti paliečiant savo kortelę terminale („bekontaktė" operacija) ir atliekant kitus veiksmus naudojant elektroninį kortelių skaitytuvą (angl*. you also give your consent to make payments from your Revolut Card by: touching your Revolut Card at the terminal (a 'contactless' transaction) and taking other actions on the electronic card reader. No PIN code is required for contactless payments up to a certain amount*).

Atsižvelgiant į tai, kad bendroji sutartis nustato bendrovės ir pareiškėjo tarpusavio santykius, bei įvertinus tai, kad mokėjimo kortelės duomenys, PIN kodo slaptažodis yra personalizuotas saugumo duomuo, kuris pripažįstamas neskelbtinu mokėjimo duomeniu (Mokėjimų įstatymo 2 straipsnio 41 dalis), darytina išvada, kad bendrojoje sutartyje nurodyti mokėjimo operacijos autorizavimo būdai – suvedant mokėjimo kortelės duomenis ir (arba) PIN kodą, paliečiant mokėjimo kortelę mokėjimo kortelių terminale, pareiškėjo ir bendrovės santykiuose laikytini pareiškėjo sutikimu įvykdyti mokėjimo operaciją tik tada, kai pats pareiškėjas pateikia mokėjimo kortelės duomenis ir (arba) suveda PIN kodo slaptažodį arba priliečia mokėjimo kortelę mokėjimo kortelių terminale norėdamas įvykdyti mokėjimo

operaciją.

Bendrovė Lietuvos bankui pateikė duomenis iš sistemų, kurie patvirtina, kad pareiškėjo ginčijamos mokėjimo operacijos kortele buvo inicijuotos pasinaudojant *Apple Pay* mokėjimo metodu, *Apple* įrenginį fiziškai pridėjus prie kasos terminalo. Tam, kad būtų galima atsiskaityti pasinaudojant *Apple Pay* mokėjimo metodu, būtina mokėjimo kortelę pridėti prie *Apple Pay* sistemos. Mokėjimo kortelės pridėjimui prie *Apple Pay* sistemos yra taikoma saugesnio autentiškumo patvirtinimo procedūra, kurios metu reikia ne tik pateikti mokėjimo kortelės duomenis, bet ir suvesti vienkartinį saugos kodą.

Bendrovės pateikti duomenys iš sistemų patvirtina, kad pareiškėjo mokėjimo kortelė prie *Apple Pay* sistemos buvo pridėta 2021 m. balandžio 15 d. 17:47:22 val., mokėjimo kortelės pridėjimą patvirtinant vienkartiniu saugos kodu.

Bendrovės iš sistemų pateiktais duomenimis, pareiškėjo mokėjimo kortelės pridėjimas prie *Apple Pay* sistemos buvo patvirtintas 2021 m. balandžio 15 d. 19:44:14 val. Nurodomas įrenginio pavadinimas – „iphone de imad". Bendrovės pateikti duomenys patvirtina, kad bendrovė 2021 m. balandžio 15 d. 16:44:05 val. telefono numeriu (*duomenys neskelbiami*) išsiuntė SMS žinutę su vienkartiniu saugos kodu. Žinutėje buvo pateikiama ši informacija: „Revolut verification code for Apple Pay (XXXXXX). Never share it whith anyone, ever". Bendrovės turimais duomenimis, bendrovės SMS žinutėje nurodytas vienkartinis saugos kodas buvo pateiktas 16:44:10 val. Šis kodas buvo suvestas tvirtinant mokėjimo kortelės pridėjimą prie *Apple Pay* sistemos. Pareiškėjas Lietuvos bankui nurodė, kad minėtos bendrovės žinutės su vienkartiniu saugos kodu nurodytu telefono numeriu jis nebuvo gavęs, mokėjimo kortelės prie *Apple Pay* sistemos jis nepridėjo ir nedavė sutikimo įvykdyti ginčijamas mokėjimo operacijas. Pareiškėjas taip pat teigė, kad apskritai nesinaudoja *Apple* įrenginiais.

Pateiktais duomenimis, telefono numeris, į kurį bendrovė pareiškėjui siuntė vienkartinį saugos kodą, kad būtų patvirtintas mokėjimo kortelės pridėjimas prie *Apple Pay* sistemos, sutampa su pareiškėjo sudarant sutartį su bendrove nurodytu telefono numeriu. Beje, tą patį telefono numerį pareiškėjas yra nurodęs ir susirašinėjime su bendrove. Pareiškėjas nei bendrovei, nei Lietuvos bankui nenurodė, kad buvo praradęs savo telefoną, priešingai, pareiškėjas Lietuvos bankui paaiškino, kad dar tą patį 2021 m. balandžio 15 d. vakarą užsisakinėjo iš *Google* paslaugas ir 18:44 val. iš bendrovės į savo telefono numerį gavo žinutę su vienkartiniu saugos kodu, kurį naudojo tik užsakydamas *Google* paslaugas. Pareiškėjas paaiškino, kad niekada niekam neatskleidžia saugos kodų, kurie jam yra atsiunčiami iš bet kurios finansų įstaigos. Vertinant pareiškėjo teiginio, kad jis į savo telefono numerį iš bendrovės negavo SMS žinutės su vienkartiniu saugos kodu, skirtu mokėjimo kortelės pridėjimui prie *Apple Pay* sistemos patvirtinti, pagrįstumą, galima teigti, kad šį pareiškėjo teiginį paneigia bendrovės pateikti įrodymai, kurie patvirtina, kad SMS žinutė su vienkartiniu saugos kodu pareiškėjo telefono numeriu buvo išsiųsta.

Pareiškėjas taip pat teigia, kad mokėjimo kortelės nebuvo praradęs ir niekam nebuvo jos perdavęs, ji atliekant ginčijamas mokėjimo operacijas buvo pareiškėjo žinioje. Pareiškėjas teigia, kad kažkas nusavino pareiškėjo mokėjimo kortelės duomenis iš bendrovės programėlės ir jais pasinaudodamas inicijavo ginčijamas mokėjimo operacijas. Pareiškėjo teigimu, tai įrodo, kad bendrovės mokėjimo sistemos yra nesaugios. Bendrovė nurodė, kad jokių techninių trikdžių atliekant ginčijamas mokėjimo operacijas nebuvo užfiksuota, taip pat nebuvo užfiksuota jokių trečiųjų asmenų įsilaužimo į pareiškėjo mokėjimo kortelės sąskaitą bendrovės programėlėje požymių.

Įvertinus pareiškėjo paaiškinimus apie ginčijamų mokėjimo operacijų atlikimo aplinkybes bei surinktus duomenis iš bendrovės sistemų kyla klausimų: jeigu darytume prielaidą, kad pareiškėjo mokėjimo kortelės duomenys, kaip teigia pareiškėjas, buvo nusavinti trečiųjų asmenų, tam, kad tretieji asmenys be pareiškėjo žinios ir sutikimo galėtų pareiškėjo mokėjimo kortelę pridėti prie *Apple Pay* sistemos ir inicijuoti ginčijamas mokėjimo operacijas, reikėjo suvesti ne tik mokėjimo kortelės duomenis, bet ir vienkartinį saugos kodą, kurį bendrovė pareiškėjui išsiuntė pareiškėjo sutartyje su bendrove nurodytu telefono numeriu. Bendrovės pateikti duomenys iš sistemų patvirtina, kad pridedant mokėjimo kortelę prie *Apple Pay* sistemos buvo suvestas bendrovės pareiškėjui SMS žinute atsiųstas vienkartinis saugos kodas. Vadinasi, jeigu, kaip teigia pareiškėjas, jis neinicijavo ginčijamų mokėjimo operacijų, tuomet tretiesiems asmenims turėjo būti žinomi ne tik mokėjimo kortelės duomenys, bet ir vienkartinis saugos kodas, skirtas mokėjimo kortelės pridėjimui prie *Apple Pay* sistemos patvirtinti, jis turėjo būti žinomas tik pareiškėjui.

Pareiškėjas teigė, kad nebuvo praradęs savo telefono ir juo dar tą patį vakarą, kurį

pareiškėjo mokėjimo kortelė buvo pridėta prie *Apple Pay* sistemos, naudojosi pats. Pareiškėjas taip pat tvirtino, kad niekam niekada neatskleidžia jokių saugos kodų, gautų iš finansinių institucijų. Vadinasi, saugos kodas, kurį pareiškėjas gavo SMS žinute į savo telefono numerį, buvo žinomas tik pareiškėjui. Kaip ir buvo minėta, pareiškėjas neigia gavęs šį vienkartinį saugos kodą į savo telefono numerį, tačiau bendrovės pateikti duomenys iš sistemų patvirtina, kad pareiškėjui bendrovė vienkartinį saugos kodą, skirtą mokėjimo kortelės pridėjimui prie *Apple Pay* sistemos patvirtinti, išsiuntė jo sutartyje su bendrove nurodytu telefono numeriu ir kad šis vienkartinis saugos kodas buvo suvestas tvirtinant mokėjimo kortelės pridėjimą prie *Apple Pay* sistemos. Taigi, įvertinus turimus duomenis, o būtent tai, kad, bendrovės pateiktais duomenimis, nebuvo užfiksuota jokių trečiųjų asmenų neteisėtų veiksmų pareiškėjo bendrovės turimoje sąskaitoje, tai, kad pareiškėjas teigė, jog mokėjimo kortelės nebuvo pametęs ir niekam nebuvo jos perdavęs, bei faktą, kad mokėjimo kortelės pridėjimas prie *Apple Pay* sistemos buvo patvirtintas ne tik suvedant mokėjimo kortelės duomenis, bet ir bendrovės pareiškėjo telefonu siųstą vienkartinį saugos kodą, kuris turėjo būti žinomas tik pareiškėjui, galima daryti išvadą, kad labiau tikėtina, kad pareiškėjo mokėjimo kortelė prie *Apple Pay* sistemos buvo pridėta gavus pareiškėjo sutikimą.

Pareiškėjas teigia, kad pats nesinaudoja *Apple* įrenginiais ir *Apple Pay* sistema, o ginčijamos mokėjimo operacijos atliktos Ispanijoje, nors šioje šalyje pareiškėjas niekada nėra buvęs, kai buvo atliekamos ginčijamos mokėjimo operacijos, pareiškėjas buvo savo namuose Maltoje. Bendrovės pateiktais duomenimis, bendrovė nėra užfiksavusi duomenų, kad pareiškėjas bendrovės išduota mokėjimo kortele, be ginčijamų mokėjimo operacijų, dar kada nors būtų atsiskaitęs Ispanijoje. Tačiau, kaip jau ir buvo nustatyta pirmiau, labiau tikėtina, kad pareiškėjo mokėjimo kortelė prie *Apple Pay* sistemos negalėjo būti pridėta be pareiškėjo žinios ir sutikimo, t. y. pareiškėjui pačiam nesuvedus arba tretiesiems asmenims neatskleidus personalizuotų saugos duomenų. Kaip ir buvo minėta, pareiškėjas neigia tretiesiems asmenims atskleidęs tiek mokėjimo kortelės duomenis, tiek vienkartinį saugos kodą ir teigia, kad mokėjimo kortelės nebuvo pametęs, niekam nebuvo jos perdavęs, o SMS žinutės su vienkartiniu saugos kodu, skirtu mokėjimo kortelei priregistruoti prie *Apple Pay* sistemos, nebuvo gavęs. Ginčo byloje taip pat nėra nustatyta jokių neteisėtų trečiųjų asmenų veiklos požymių, kad tretieji asmenys galėjo pasisavinti pareiškėjo mokėjimo kortelės duomenis bei vienkartinį saugos kodą ir be pareiškėjo žinios ir sutikimo inicijuoti ginčijamas mokėjimo operacijas, todėl nėra pagrindo vertinti pareiškėjo kaltės formos, t. y. vertinti, ar pareiškėjas mokėjimo priemonę prarado tyčia, ar dėl didelio neatsargumo neįvykdęs vienos ar kelių Mokėjimų įstatymo 34 straipsnyje nustatytų pareigų.

Nepaisant to, kad pareiškėjas teigia, jog atliekant ginčijamas mokėjimo operacijas buvęs Maltoje, o ne Ispanijoje ir pats mokėjimo kortelės *Apple Pay* sistemoje nepriregistravo ir nepridėjo *Apple* įrenginio prie kasos terminalo, tačiau, kaip jau minėta, surinkti duomenys leidžia daryti labiau tikėtiną išvadą, kad be pareiškėjo žinios ir sutikimo pareiškėjo mokėjimo kortelė negalėjo būti pridėta prie *Apple Pay* sistemos. Mokėjimo kortelę pridėjus prie *Apple Pay* sistemos ir pridėjimą patvirtinus saugos kodu, yra įgyjama galimybė naudotis mokėjimo kortele kaip sava, jos fiziškai neturint, o mokėjimo operacijas tvirtinant pridėjus *Apple* įrenginį. Bendrovės Lietuvos bankui pateikti duomenys patvirtina, kad abi ginčijamos mokėjimo operacijos buvo įvykdytos pasinaudojant pareiškėjo mokėjimo kortele ir fiziškai pridėjus *Apple* įrenginį prie kasos terminalo.

Kaip ir buvo minėta, pareiškėjui teigiant, kad jis neprarado mokėjimo kortelės bei niekam neatskleidė bendrovės pareiškėjo ir bendrovės sutartyje nurodytu telefono numeriu išsiųsto vienkartinio saugos kodo, esant objektyviems duomenims, kad pareiškėjo mokėjimo kortelė prie *Apple Pay* sistemos buvo pridėta laikantis saugesnio autentiškumo patvirtinimo reikalavimų (suvesti ne tik mokėjimo kortelės duomenys, bet ir vienkartinis saugos kodas), taip pat atsižvelgiant į tai, kad pareiškėjo ir bendrovės sutartyje buvo sutarta dėl mokėjimo operacijų kortele autorizavimo tvarkos, kaip yra pateikiami mokėjimo kortelės duomenys ir (arba) PIN kodo slaptažodis, taip pat nesant jokių objektyvių duomenų, kad tretieji asmenys neteisėtu būdu būtų pasisavinę pareiškėjo mokėjimo priemonę ir tik vienam pareiškėjui žinomą vienkartinį saugos kodą ir be pareiškėjo žinios mokėjimo kortelę būtų pridėję prie *Apple Pay* sistemos ir taip įgiję galimybę inicijuoti mokėjimo operacijas pasinaudojant pareiškėjo mokėjimo kortele, nėra pagrindo vertinti, kad pareiškėjo ginčijamos mokėjimo operacijos gali būti laikomos neautorizuotomis. Atitinkamai darytina išvada, kad bendrovė neturi pareigos pareiškėjui grąžinti mokėjimo operacijų, kurios buvo patvirtintos bendrovės ir pareiškėjo sutartyje sutarta tvarka ir bendrovės tinkamai įvykdytos, lėšas. Atsižvelgiant į tai, darytina

išvada, kad pareiškėjo reikalavimas bendrovei grąžinti ginčijamų mokėjimo operacijų sumą – 200 Eur, yra nepagrįstas, todėl atmestinas.

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:

Atmesti pareiškėjo X.X. reikalavimą.

Lietuvos banko sprendimas dėl ginčo esmės yra rekomendacinio pobūdžio ir teismui neskundžiamas. Vartotojui ir finansų rinkos dalyviui išlieka teisė dėl ginčo sprendimo kreiptis į teismą arba kitą ginčų nagrinėjimo instituciją įstatymų nustatyta tvarka. Kreipimasis į teismą po Lietuvos banko sprendimo dėl ginčo esmės priėmimo nelaikomas šio sprendimo apskundimu.

Direktorius Arūnas Raišutis