LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

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

[Data] Nr. [Nr.]
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:

2022 m. spalio 12 d. iš pareiškėjos sąskaitos banke pareiškėjai banko išduota mokėjimo kortele buvo inicijuotos 7 mokėjimo operacijos gavėjui *Monodirect* (toliau – gavėjas). Bendra mokėjimo operacijų suma – 4 548,89 GPB (toliau – mokėjimo operacijos). Mokėjimo operacijos buvo inicijuotos pareiškėjos mokėjimo kortelę pridėjus prie elektroninės piniginės panaudojant *Apple Pay* atsiskaitymo metodą.

Bankui atsisakius pareiškėjai grąžinti mokėjimo operacijų sumą, pareiškėja kreipėsi į Lietuvos banką dėl vartojimo ginčo nagrinėjimo.

Kreipimesi pareiškėja paaiškino, kad 2022 m. spalio 12 d. naudodamasi *Vinted* programėle gavo pranešimą, kuriame buvo prašoma suvesti mokėjimo kortelės duomenis, kad būtų patvirtintas lėšų už paduodamą prekę įskaitymas į pareiškėjos banko sąskaitą. Pareiškėja paspaudė jai trečiųjų asmenų pateiktą aktyvią nuorodą ir suvedė savo mokėjimo kortelės duomenis. Pareiškėja teigė, kad iš karto po to, kai suvedė mokėjimo kortelės duomenis, pastebėjo, kad iš jos sąskaitos banke buvo įvykdytos mokėjimo operacijos. Pareiškėja nedelsdama kreipėsi į banką ir prašė sustabdyti mokėjimo operacijų vykdymą, tačiau, nepaisydamas pareiškėjos prašymo, bankas mokėjimo operacijas įvykdė. Pareiškėja prašė rekomenduoti bankui grąžinti 4 548,89 GPB mokėjimo operacijų sumą.

Bankas Lietuvos bankui pateiktame atsiliepime paaiškino, kad mokėjimo operacijos buvo inicijuotos pareiškėjos mokėjimo kortelę pridėjus prie *Apple Pay* ir konkrečią mokėjimo operaciją patvirtinus panaudojant *Apple Pay* mokėjimo metodą. Banko sistemų duomenimis, pareiškėjos mokėjimo kortelė prie *Apple Pay* buvo pridėta suvedus mokėjimo kortelės duomenis (kortelės numerį, galiojimo datą ir kortelės saugos kodą – CVV) ir mokėjimo kortelės pridėjimą patvirtinus įvedant vienkartinį saugos kodą, gautą trumpąja SMS žinute. Bankas pažymėjo, kad SMS žinutė su vienkartiniu saugos kodu buvo siunčiama į telefono numerį, kuris buvo nurodytas pareiškėjos sudarant sutartį su banku. Be to, pareiškėja nenurodė, kad ji buvo pametusi savo mobilųjį telefoną ar kad jis galėjo būti ne pareiškėjos žinioje. Kartu su vienkartiniu saugos kodu pareiškėjai SMS žinutėje buvo nurodyta ir šio kodo paskirtis bei perspėjimas šio kodo neperduoti tretiesiems asmenims.

Papildomai bankas atkreipė dėmesį į tai, kad, pareiškėjai inicijuojant pirmąją mokėjimo operaciją, banko kontrolės sistemos operaciją atmetė dėl galimai įtartino jos pobūdžio, o pareiškėjos mokėjimo kortelė banko sistemų buvo užblokuota. Be to, bankas pareiškėjai SMS žinute išsiuntė įspėjimą dėl įtartinos mokėjimo operacijos, tačiau pareiškėja šio įspėjimo nepaisė ir pati atblokavo savo mokėjimo kortelę.

Taip pat bankas pažymėjo, kad pareiškėjos veiksmai, dėl kurių ji prarado savo mokėjimo

[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*.

priemonę, gali būti vertinamai kaip labai neatsargūs, nes tretieji asmenys be pareiškėjos žinios galėjo inicijuoti mokėjimo operacijas tik dėl to, kad pareiškėja dėl didelio neatsargumo neįvykdė Lietuvos Respublikos mokėjimų įstatymo 34 straipsnyje bei banko Privatiems klientams taikomose sąlygose įtvirtintų mokėtojo pareigų. Pareiškėja neišsaugojo mokėjimo kortelės duomenų konfidencialumo – nesiėmė saugumo priemonių, kurių privalėjo imtis, kad būtų tinkamai apsaugoti jai suteiktos mokėjimo kortelės duomenys, ir tretiesiems asmenims suteikė (nurodė) vienkartinį saugos kodą, kurį gavo į jai priklausantį telefono numerį trumpąja SMS žinute. Banko teigimu, pareiškėja nors ir neigia tretiesiems asmenims atskleidusi SMS žinute gautą vienkartinį saugos kodą, kuriuo ir buvo patvirtintas mokėjimo kortelės pridėjimas prie *Apple Pay,* tačiau be šio kodo panaudojimo mokėjimo kortelės pridėjimas prie *Apple Pay* yra neįmanomas, todėl, banko nuomone, pareiškėja perdavė šį kodą tretiesiems asmenims, tai ir lėmė mokėjimo operacijų iš pareiškėjos sąskaitos įvykdymą.

Atsižvelgdamas į visas pirmiau nurodytas aplinkybes, bankas prašė atmesti pareiškėjos reikalavimą kaip nepagrįstą.

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

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

Pareiškėjos ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjai pareiškėjos vardu banke atidarytoje sąskaitoje mokėjimo kortele atliktų mokėjimo operacijų lėšas, iš viso 4 548,89 GPB. Pareiškėja teigia neautorizavusi (nenorėjusi įvykdyti) mokėjimo operacijų, tačiau ir neneigia trečiųjų asmenų suklastotame *Vinted* interneto puslapyje pati suvedusi savo mokėjimo kortelės duomenis. Tačiau pareiškėja neigia tretiesiems asmenims atskleidusi banko SMS žinute gautą vienkartinį saugos kodą, kuriuo buvo patvirtintas mokėjimo kortelės pridėjimas prie *Apple Pay.* Pareiškėja taip pat teigia, kad tuo metu, kai kreipėsi į banką ir prašė blokuoti jos mokėjimo kortelę, mokėjimo operacijų lėšos pareiškėjos sąskaitoje buvo dar tik rezervuotos, todėl bankas galėjo atšaukti mokėjimo operacijų įvykdymą ir grąžinti pareiškėjai mokėjimo operacijų lėšas.

Bankas teigia, kad pareiškėjos mokėjimo operacijos buvo patvirtintos šalių sutarta forma ir tvarka, dėl to bankas jas pagrįstai įvykdė, o pareiškėja į banką dėl mokėjimo operacijų atšaukimo kreipėsi po to, kai mokėjimo nurodymai buvo gauti banke, todėl bankas mokėjimo operacijų be gavėjo sutikimo atšaukti negalėjo. Taip pat bankas teigia, kad yra sąlygos pareiškėjos elgesį, prarandant savo mokėjimo priemonę, vertinti kaip labai neatsargų, todėl mano, kad neturi pareigos kompensuoti pareiškėjai jos patirtų nuostolių dėl mokėjimo operacijų įvykdymo. Dėl šių priežasčių, banko nuomone, visi mokėjimo operacijų nuostoliai turėtų tekti pareiškėjai.

Tarp šalių nėra ginčo, kad nebuvo duotas pareiškėjos sutikimas vykdyti mokėjimo operacijas, t. y. tiek pareiškėja, tiek bankas pripažįsta, kad mokėjimo operacijas inicijavo ne pati pareiškėja, o tretieji asmenys, neteisėtu būdu pasisavinę pareiškėjos mokėjimo priemonę. Atsižvelgiant į tai, kad iš esmės abi ginčo šalys sutaria, kad mokėjimo operacijos galėjo būti inicijuotos be pačios pareiškėjos valios, o trečiųjų asmenų iniciatyva, toliau sprendime nebus analizuojamos su mokėjimo operacijų autorizavimo vertinimu susijusios aplinkybės, o mokėjimo operacijos laikomos pareiškėjos neautorizuotomis.

Ginčo šalys iš esmės nesutaria dėl to, kam turėtų tekti atsakomybė už neautorizuotų mokėjimo operacijų įvykdymą: bankas teigia, kad pareiškėjos elgesys, tretiesiems asmenims atskleidžiant savo personalizuotus saugos duomenis ir prarandat savo mokėjimo priemonę, buvo labai neatsargus. Pareiškėja neneigia pati trečiųjų asmenų suklastotame *Vinted* platformos puslapyje suvedusi savo mokėjimo kortelės duomenis, tačiau teigia, kad bankas jai kreipusis dėl mokėjimo operacijų atšaukimo turėjo jas atšaukti ir pareiškėjai sugrąžinti mokėjimo operacijų lėšas.

Siekiant išspręsti tarp pareiškėjos ir banko kilusį ginčą, Lietuvos banko vertinimu, būtina nustatyti šias pagrindines aplinkybes: 1) ar bankas turėjo (turi) pareigą grąžinti pareiškėjai neautorizuotų mokėjimo operacijų sumas; 2) ar bankas turėjo pareigą atšaukti mokėjimo

operacijas.

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.

1. Dėl neautorizuotų mokėjimo operacijų pasekmių ir pareiškėjos teisės į mokėjimo operacijų sumų grąžinimą

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

Pagal Mokėjimų įstatymo 39 straipsnio 1 dalį, mokėtojui gali tekti dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai iki 50 eurų, kai šie nuostoliai patirti dėl: 1) prarastos ar pavogtos mokėjimo priemonės panaudojimo; 2) neteisėto mokėjimo priemonės pasisavinimo. Tačiau, kaip nustatyta Mokėjimų įstatymo 39 straipsnio 2 dalyje, mokėtojas neturi patirti jokių nuostolių, jeigu jis iki mokėjimo operacijos įvykdymo negalėjo pastebėti mokėjimo priemonės praradimo, vagystės arba neteisėto pasisavinimo, išskyrus atvejus, kai jis veikė nesąžiningai (1 punktas).

Mokėjimų įstatymo 39 straipsnio 3 dalyje nustatyta, kad mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai, jeigu jis juos patyrė veikdamas nesąžiningai arba tyčia ar dėl didelio neatsargumo neįvykdęs vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų. Tokiais atvejais Mokėjimų įstatymo 39 straipsnio 1 dalyje nustatytas didžiausios nuostolių sumos ribojimas netaikomas.

Pagal Mokėjimų įstatymo 2 straipsnio 32 dalį, mokėjimo priemonė – personalizuota priemonė ir (arba) tam tikros procedūros, dėl kurių susitaria mokėjimo paslaugų vartotojas ir mokėjimo paslaugų teikėjas ir kurias mokėjimo paslaugų vartotojas naudoja mokėjimo nurodymui inicijuoti. Pasisavinimas šiuo atveju turėtų būti suprantamas kaip svetimos mokėjimo priemonės užvaldymas ir galėjimas ja naudotis kaip sava. Neteisėtumas suponuoja atlikto veiksmo teisinio pagrindo nebuvimą.

Bankas teigia, kad tretieji asmenys neteisėtu būdu galėjo pasisavinti pareiškėjos mokėjimo kortelės duomenis bei kitus personalizuotus saugos duomenis tik todėl, kad pareiškėja dėl savo didelio neatsargumo neįvykdė Mokėjimų įstatymo 34 straipsnyje numatytų mokėtojo pareigų ir neužtikrino, kad, be pareiškėjos, turinčios teisę naudotis mokėjimo priemone, personalizuotais saugumo duomenimis negalėtų pasinaudoti kiti asmenys.

Ginčo byloje nustatyta, kad pareiškėja prarado savo mokėjimo priemonę, kai per *Vinted* platformą su ja susiekė tariamas pareiškėjos parduodamos prekės pirkėjas ir paprašė jos pasidalinti savo mokėjimo kortelės duomenimis, kad lėšos už parduodamą prekę būtų įskaitytos į pareiškėjos banko sąskaitą. Pareiškėja teigė, kad jos buvo prašoma patvirtinti lėšų įskaitymo į jos sąskaitą mokėjimo operaciją. Pareiškėja nei bankui, nei Lietuvos bankui nepateikė ekrano vaizdo, kurį ji matė, prieš vesdama savo mokėjimo kortelės duomenis, kopijos.

Banko pateiktais duomenimis, 2022 m. spalio 12 d. 16:29:01 val. pareiškėja savo mobiliojo telefono numeriu iš banko gavo SMS žinutę su tokiu pranešimo testu: *„Revolut verification code for Apple Pay:191328. This code will be used to add card to another Apple Pay device. Never share it whith anyone and don;t enter it anywhere unless you want to add your card to another device.*" Pareiškėja neigia šį kodą atskleidusi tretiesiems asmenims, tačiau banko pateikti duomenys įrodo, kad vienkartinis saugos kodas buvo siųstas į pareiškėjos bankui nurodytą telefono numerį ir kad jis buvo panaudotas mokėjimo kortelei pridėti prie *Apple Pay.* Pareiškėja teigė, kad mobilusis telefonas visą laiką buvo jos žinioje. Vadinasi, niekas kitas be pačios pareiškėjos vienkartinio saugos kodo duomenų negalėjo žinoti ir jų perduoti tretiesiems asmenims.

Pagal ginčo byloje pareiškėjos pateiktus paaiškinimus, spausdama trečiųjų asmenų jai atsiųstoje žinutėje pateiktą aktyvią nuorodą ir vesdama savo kortelės duomenis ji tikėjosi už prekę gauti pinigus į savo sąskaitą banke. Teigdamas, kad pareiškėjos elgesys, dėl kurio ji prarado savo mokėjimo priemonę, turi didelio neatsargumo požymių, bankas remiasi tuo, kad

pareiškėja nesilaikė mokėtojui nustatytos pareigos saugoti personalizuotus saugos duomenis ir niekam jų neatskleisti.

Lietuvos bankas pažymi, kad didelis neatsargumas ar paprastas neatsargumas yra vertinamojo pobūdžio aplinkybės, todėl išvada dėl mokėtojo elgesio vertinimo kaip neatsargaus ar labai neatsargaus dėl neautorizuotos mokėjimo operacijos ar dėl mokėjimo priemonės praradimo, lėmusio neautorizuotą mokėjimo operaciją, darytina kiekvienu konkrečiu atveju, įvertinus nustatytų individualių, specifinių aplinkybių visumą, kurią patvirtina ginčo byloje esantys įrodymai ir (arba) yra šalių neginčijamos neautorizuotos mokėjimo operacijos įvykdymo aplinkybės. 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 (toliau – PSD2) 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).

Vertinant pareiškėjos veiksmus, kuriais, kaip pati pareiškėja pripažįsta, tretiesiems asmenims perdavė savo mokėjimo kortelės duomenis, turėdama tikslą, kad lėšos už jos parduodamą prekę būtų įskaitytos į jos banko sąskaitą, visų pirma pažymėtina, kad tam, kad lėšos būtų įskaitytos į banko sąskaitą, nereikia suvesti mokėjimo kortelės duomenų. Priešingai, mokėjimo kortelės duomenys yra reikalingi tam, kad būtų inicijuotas mokėjimo operacijos iš banko sąskaitos vykdymą. Norint gauti pinigines lėšas į savo banko sąskaitą, bankai neprašo tuo tikslu tretiesiems asmenims pateikti savo mokėjimo kortelės duomenų, SMS žinute nesiunčia vienkartinio saugos kodo ir neprašo jo suvesti siekiant mokėjimo kortelę pridėti prie *Apple Pay*. Tačiau pareiškėjai faktas, kad tam, kad lėšos būtų pervestos į jos sąskaitą, jos buvo prašoma suvesti duomenis, kurie iš esmės yra reikalingi atlikti priešingą veiksmą – patvirtinti lėšų iš banko sąskaitos nurašymą, nesukėlė jokių įtarimų ir pareiškėja vykdė trečiųjų asmenų nurodymus jų nevertindama kritiškai.

Svarbu pažymėti, kad, banko pateiktais duomenimis, banko pareiškėjai siųstoje SMS žinutėje su vienkartiniu saugos kodu, skirtu pridėti mokėjimo kortelę prie *Apple Pay*, buvo aiškiai pateikta informacija, kokiu tikslu saugos kodas yra siunčiamas, kur jis bus naudojamas ir pareiškėja netgi buvo perspėta, kad šiuo kodu nesidalintų ir niekur jo nevestų, jeigu neturima tikslo mokėjimo kortelę pridėti prie *Apple Pay.*

Taigi, pareiškėjai turėjo sukelti įtarimų ne tik tas faktas, kad lėšoms į sąskaitą įskaityti prašoma suvesti mokėjimo kortelės duomenis, bet ir minėta SMS žinutėje banko pareiškėjai pateikta informacija, todėl pareiškėja turėjo kritiškai vertinti savo tolimesnius veiksmus ir nuo jų susilaikyti.

Nors pareiškėja ir neigia, kad kam nors atskleidė SMS žinute gautą vienkartinį saugos kodą, tačiau ginčo bylos duomenys patvirtina, kad pareiškėjos mokėjimo kortelė buvo pridėta prie *Apple Pay* suvedus SMS žinute pareiškėjos telefono numeriu siųstą vienkartinį saugos kodą. Ginčo byloje nėra duomenų, kad pareiškėjos telefonu būtų naudojęsi tretieji asmenys, tai leidžia teigti, kad pati pareiškėja tretiesiems asmenims perdavė ne tik mokėjimo kortelės duomenis, tai pareiškėja pripažįsta, bet ir SMS žinute gautą vienkartinį saugos kodą. Jeigu šio SMS žinute siųsto vienkartinio saugos kodo pareiškėja nebūtų atskleidusi, mokėjimo kortelė nebūtų galėjusi būti pridėta prie *Apple Pay* ir mokėjimo operacijos nebūtų buvę įvykdytos. Tačiau pareiškėja nekreipė dėmesio į šią banko žinutę, kurioje iš esmės buvo aiškiai parašytas vienkartinio saugos kodo siuntimo tikslas – pridėti mokėjimo kortelę prie *Apple Pay*, o ne įskaityti mokėjimo operacijos lėšas, kaip manė pareiškėja, ir toliau tęsė neatsargius veiksmus.

Banko pateiktais duomenimis, pačią pirmą mokėjimo operaciją bankas atmetė, užblokavo pareiškėjos mokėjimo kortelę ir pareiškėjai išsiuntė SMS žinutę, kurioje įspėjo, kad

inicijuojama mokėjimo operacija yra įtartina ir gali būti susijusi su sukčiavimu. Tačiau pareiškėja nepaisė ir šios banko pateiktos informacijos ir pati atblokavo mokėjimo kortelę, tai lėmė tolimesnių mokėjimo operacijų iš pareiškėjos sąskaitos vykdymą.

Banko Privatiems klientams taikomų sąlygų (toliau – Sąlygos) 14 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. <...>"

Kaip matyti, banko mokėjimo pasaugų teikimo sąlygos aiškiai reglamentuoja, kad banko klientui suteiktų personalizuotų duomenų naudojimas yra skirtas duoti sutikimą įvykdyti mokėjimo operaciją. Ginčo byloje nėra duomenų, kad pareiškėja būtų buvusi nesupažindinta su Sąlygomis ar kad būtų jų nesupratusi. Taigi, pareiškėja iš esmės galėjo suprasti, kad mokėjimo kortelės duomenų suvedimas gali lemti tam tikras teisines pasekmes, šiuo atveju – mokėjimo priemonės praradimą ir neautorizuotų mokėjimo operacijų iš jos banko sąskaitos įvykdymą.

Lietuvos banko nuomone, jeigu pareiškėja būtų buvusi pakankamai atidi ir kritiška tiek trečiųjų asmenų žinute gautos informacijos atžvilgiu, tiek ir savo atliekamų veiksmų atžvilgiu, būtų pastebėjusi, kad jos prašoma atlikti veiksmus, kurių nėra įprastai prašoma atlikti norint pinigines lėšas gauti į savo sąskaitą, o priešingai – yra prašoma atlikti veiksmus, kurie įprastai yra atliekami norint įvykdyti mokėjimo operacijas iš banko sąskaitos. Banko pareiškėjai siųstoje SMS žinutėje su vienkartiniu saugos kodu buvo aiškiai nurodyta, kad vienkartinis saugos kodas yra skirtas mokėjimo kortelę pridėti prie *Apple Pay*. Banko Lietuvos bankui pateiktais duomenimis, pareiškėja pati naudojosi *Apple Pay* mokėjimo metodu, todėl galėjo suprasti *Apple Pay* mokėjimo metodo paskirtį, o ir faktas, kad pareiškėjos yra prašoma pridėti mokėjimo kortelę prie naujame įrenginyje įdiegto *Apple Pay*, turėjo pareiškėjai sukelti įtarimų ir pareiškėja turėjo susilaikyti nuo tolimesnių veiksmų.

Jeigu pareiškėja būtų buvusi pakankamai atidi ir rūpestinga savo su mokėjimo priemone atliekamų veiksmų atžvilgiu, ji būtų galėjusi pastebėti trečiųjų asmenų neteisėtus veiksmus ir, labai tikėtina, būtų išvengusi neautorizuotų mokėjimo operacijų iš jos banko sąskaitos įvykdymo. Vis dėlto pareiškėja elgėsi nerūpestingai ir toliau vykdė trečiųjų asmenų jai pateiktus nurodymus. Lietuvos banko vertinimu, pareiškėjos elgesys gali būti pripažintas kaip elgesys, iš esmės besiskiriantis nuo atsargaus elgesio reikalavimų, jis galiausiai ir lėmė tai, kad pareiškėja prarado savo mokėjimo priemonę, o tretieji asmenys įgijo galimybę pareiškėjos vardu inicijuoti mokėjimo operacijas.

Mokėjimų įstatymo 34 straipsnyje reglamentuojamos mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigos: 1) naudotis mokėjimo priemone pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas; 2) sužinojus apie mokėjimo priemonės praradimą, vagystę arba neteisėtą pasisavinimą ar neautorizuotą jos naudojimą, nedelsiant apie tai pranešti mokėjimo paslaugų teikėjui arba jo nurodytam subjektui. Mokėjimo paslaugų vartotojas, gavęs mokėjimo priemonę, privalo imtis veiksmų, kad būtų apsaugoti personalizuoti saugumo duomenys (2 dalis).

Taigi, įvertinus ginčo byloje turimus duomenis bei ginčo šalių paaiškinimus apie mokėjimo operacijų įvykdymo aplinkybes, galima teigti, kad pareiškėja mokėjimo priemone naudojosi nesilaikydama mokėjimo priemonės išdavimą ir naudojimą reglamentuojančių sąlygų ir neįvykdė Mokėjimų įstatymo 34 straipsnyje reglamentuojamų mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigų.

Visų ginčo byloje nustatytų aplinkybių kontekste galima daryti išvadą, kad pareiškėjos veiksmai, dėl kurių ji prarado mokėjimo priemonę, pasireiškė dideliu neatsargumu, tai galiausiai ir lėmė, kad buvo įvykdytos neautorizuotos mokėjimo operacijos iš pareiškėjos sąskaitos ir pareiškėja patyrė nuostolių.

Mokėjimų įstatymo 39 straipsnio 3 dalyje nustatyta, kad mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai, jeigu jis juos patyrė veikdamas nesąžiningai arba tyčia ar dėl didelio neatsargumo neįvykdęs vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų. Įvertinus pirmiau išdėstytą informaciją, konstatuotina, kad yra pagrindas pareiškėjai taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, todėl pareiškėjos reikalavimas bankui grąžinti neautorizuotų mokėjimo operacijų lėšų sumą yra nepagrįstas ir atmestinas.

2. Dėl mokėjimo operacijų įvykdymo pagrįstumo bei mokėjimo nurodymų įvykdyti mokėjimo operacijas atšaukimo

Pareiškėja teigė, kad bankas turėjo atšaukti mokėjimo operacijas, nes ji, vos tik pastebėjusi, kad iš jos sąskaitos be jos sutikimo yra vykdomos mokėjimo operacijos, kreipėsi į banką ir prašė šias mokėjimo operacijas atšaukti.

Vertinant banko pareigos atšaukti mokėjimo operacijas vykdymą, pažymėtina, kad, pagal Mokėjimų įstatymo 44 straipsnio 1 dalies nuostatas, mokėjimo paslaugų vartotojas negali atšaukti mokėjimo nurodymo po to, kai jį gauna mokėtojo mokėjimo paslaugų teikėjas, išskyrus šiame straipsnyje nustatytas išimtis. Minėto Mokėjimų įstatymo straipsnio 4 dalyje taip pat nustatyta, kad, pasibaigus 1 dalyje nurodytam laikotarpiui, mokėjimo nurodymas gali būti atšauktas tik tuo atveju, kai dėl to susitaria mokėjimo paslaugų vartotojas ir atitinkamas mokėjimo paslaugų teikėjas, o šio straipsnio 2 dalyje numatytais atvejais būtinas ir gavėjo sutikimas. Mokėjimo paslaugų teikėjas gali imti komisinį atlyginimą už mokėjimo nurodymo atšaukimą, jeigu tai numatyta bendrojoje sutartyje.

Taigi, pasibaigus Mokėjimų įstatymo 44 straipsnio 1 dalyje nurodytam terminui, mokėjimo nurodymas gali būti atšauktas tik dėl to susitarus vartotojui ir jo mokėjimo paslaugų teikėjui, todėl nurodytos galimybės (t. y. mokėjimo nurodymo atšaukimo) įtvirtinimas Mokėjimų įstatyme neturėtų būti vertinamas kaip priverstinis lėšų grąžinimas mokėtojui, esant jo atitinkamam prašymui (pasibaigus 44 straipsnio 1 dalyje nurodytam terminui).

Remiantis ginčo byloje esančiais duomenimis, pareiškėjos prašymas atšaukti mokėjimo operacijas bankui buvo pateiktas po to, kai mokėjimo nurodymus jau buvo gavęs bankas, todėl Mokėjimų įstatyme nustatyta mokėjimo nurodymo atšaukimo terminas jau buvo praėjęs ir bankas atšaukti pareiškėjos vardu pateiktų mokėjimo nurodymų nebegalėjo.

Taip pat bankas paaiškino, kad lėšų grąžinimo prašymas nepateko į mokėjimo kortelių organizacijos „Mastercard" apibrėžtas ginčytinų mokėjimo operacijų kategorijas, todėl lėšų grąžinimo procedūra „Mastercard" nustatyta tvarka taip pat negalėjo būti inicijuota.

Atsižvelgiant į tai, kas buvo išdėstyta pirmiau, nėra pagrindo vertinti, kad bankas nepagrįstai įvykdė mokėjimo operacijas ir kad nepagrįstai jų neatšaukė.

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 pareiškėjos 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.

[Pareigų pavadinimas] [Vardas ir pavardė]