LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

SPRENDIMAS DĖL X.X. IR *LUMINOR BANK AS* GINČO NAGRINĖJIMO

2023-05-17 Nr. 429-290
Vilnius

Lietuvos bankas gavo X.X. (toliau – pareiškėjas) kreipimąsi, kuriuo prašoma išnagrinėti tarp pareiškėjo ir banko *Luminor Bank AS*, veikiančio per Lietuvoje įsteigtą skyrių, (toliau – bankas) kilusį ginčą.

N u s t a t y t a:

2022 m. balandžio 19 – 20 d. iš pareiškėjo sąskaitos banke pareiškėjui banko išduota mokėjimo kortele panaudojant *Apple Pay* mokėjimo operacijos patvirtinimo metodą buvo inicijuota ir patvirtinta 12 mokėjimo operacijų šiems gavėjams: *LA CIVETTE ST PARIS FR*, *SNCF COLOMBES FR*, *TABAC DE LA GAR COLOMBES FR*; (toliau – gavėjai), kurių bendra suma – 2 263,95 Eur (toliau – mokėjimo operacijos). Mokėjimo operacijos buvo įvykdytos pareiškėjo mokėjimo kortelę pridėjus prie *Apple Pay* įdiegto kitame įrenginyje.

Bankui atsisakius pareiškėjui grąžinti mokėjimo operacijų sumą, pareiškėjas kreipėsi į Lietuvos banką prašydamas išnagrinėti vartojimo ginčą ir grąžinti visą mokėjimo operacijų sumą. Pareiškėjas paaiškino, kad „2022 metų balandžio 19-20 dienomis apgaulės būdu iš Luminor banke esančios mano sąskaitos Nr. *duomenys neskelbiami* per kelis kartus buvo nurašyti 2 263,95 Eur. Buvo kreiptasi į Luminor banką dėl įvykio aplinkybių išsiaiškinimo, kadangi pinigai buvo nurašyti *Apple Pay* mokėjimo priemonės pagalba, kurios aš pats nei sukūriau, nei tvirtinau. Luminor bankas nesutiko su mano teiginiais ir patarė kreiptis į policiją < >. Ikiteisminis tyrimas patvirtino, kad 2022 m. balandžio 19 d. į mano mob. telefono numerį iš Luminor banko buvo siųstos trys SMS žinutės, iš kurių viena buvo tokia: 2022 04 19 13:55 val. „Įveskite kodą *duomenys neskelbiami* norėdami pridėti kortelę į skaitmeninę piniginę. Šis kodas galioja 30 minučių", tačiau nebuvo pateikta įrodymų, kad tos žinutės buvo gautos į mano mobilųjį telefoną. Tuo tarpu mano mob. telefono išklotinė įrodo, kad nei viena iš Luminor banko siųstų žinučių nebuvo gauta. Vadinasi, sukčiai pasinaudojo Luminor banko saugos sistemos spraga, kadangi galimai trumpųjų žinučių siuntėjo duomenys nebuvo realūs, o buvo tranzitiniai, apeinant mobiliojo ryšio operatorių „Bitė Lietuva". Luminor banko *Apple Pay* mokėjimo verifikacijos kodas pateko tiesiai sukčiams, kurie jį ir suvedė į sistemą bei pasinaudojo mokėjimo priemone, nurašydami pinigus iš mano sąskaitos".

Ginčo nagrinėjimo metu, pareiškėjas Lietuvos bankui papildomai paaiškino, kad 2022 m. balandžio 19 d. jis elektroniniu paštu neva iš *LP Express* gavo žinutę, kurioje buvo prašoma paspausti aktyvią nuorodą ir sumokėti 1,90 Eur už siuntos pristatymo išlaidas. Šiuo tikslu pareiškėjas ir suvedė savo mokėjimo kortelės duomenis. Pareiškėjas teigė, kad panašių laiškų dėl ateinančių siuntų jis gaudavo kasdien, todėl jam nekilo joks įtarimas, kad tai gali būti apgaulė. Pareiškėjas taip pat teigė, kad bankas nesiėmė jokių prevencijos priemonių sukčiavimui užkardyti ir pareiškėjo neinformavo apie tai, kad prie pareiškėjo banko sąskaitos buvo prisijungta iš kito įrenginio.

Bankas Lietuvos bankui pateiktame atsiliepime paaiškino, kad pareiškėjas dėl didelio neatsargumo neišsaugojo savo personalizuotų saugos duomenų, todėl tretieji asmenys jais galėjo pasinaudoti ir be pareiškėjo žinios inicijuoti mokėjimo operacijas. Banko teigimu, mokėjimo operacijos buvo įvykdytos pareiškėjo mokėjimo kortelę susiejus su skaitmenine pinigine (*Apple Pay*), kortelės susiejimą patvirtinus suvedant banko pareiškėjui mobiliuoju telefonu išsiųstą vienkartinį saugos kodą. Bankas pažymėjo, kad pareiškėjas iš trečiųjų asmenų elektroniniu paštu gavęs pranešimą su aktyvia nuoroda, kur jo buvo prašoma sumokėti

1,90 Eur neva už siuntos pristatymą, šiuo tikslu suvedė savo mokėjimo kortelės duomenis, kuriuo tretieji asmenys nusavino ir panaudojo pareiškėjo mokėjimo kortelę pridedant prie *Apple Pay.*

Bankas paaiškino, kad dėl pareiškėjo teiginio, jog „trumpųjų žinučių siuntėjo duomenys nebuvo realūs, o tranzitiniai – apeinant UAB „Bitė Lietuva" negali pakomentuoti, nes remiasi savo naudojamų sistemų duomenimis, kurie įrodo, kad SMS žinutė su vienkartiniu saugos kodu buvo išsiųsta į pareiškėjo mobiliojo telefono numerį.

Atsižvelgdamas į visas pirmiau nurodytas aplinkybes, bankas prašė atmesti pareiškėjo 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. 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 galimai padarytu Lietuvos banko kompetencijai priskirtų teisės aktų reikalavimų pažeidimu, nustatyti ir įvertinti. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Pareiškėjo ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjui pareiškėjo vardu banke atidarytoje sąskaitoje kortele atliktų mokėjimo operacijų lėšas, iš viso 2 263,95 Eur. Pareiškėjas teigia neautorizavęs mokėjimo operacijų, tačiau pripažįsta trečiųjų asmenų suklastotame *LP Express* interneto puslapyje suvedęs savo mokėjimo kortelės duomenis. Visgi pareiškėjas neigia iš banko savo telefono numeriu gavęs SMS žinutę su vienkartiniu saugos kodu, skirtu mokėjimo kortelę pridėti prie *Apple Pay.* Pareiškėjo teigimu, sukčiai pasinaudojo banko saugumo sistemos spragomis, tokiu būdu SMS žinutė su vienkartiniu saugos kodu buvo išsiųsta tiesiogiai sukčiams. Bankas teigia, kad pareiškėjo mokėjimo operacijos buvo patvirtintos šalių sutarta forma ir tvarka, dėl to bankas jas pagrįstai įvykdė. Taip pat bankas teigia, kad yra sąlygos pareiškėjo elgesį, prarandant savo mokėjimo priemonę, vertinti kaip labai neatsargų, todėl bankas mano, kad neturi pareigos kompensuoti pareiškėjui jo patirtų nuostolių dėl įvykdytų mokėjimo operacijų. Dėl šių priežasčių, banko nuomone, visi mokėjimo operacijų nuostoliai turėtų tekti pareiškėjui.

Siekdamas išspręsti tarp šalių kilusį ginčą ir įvertinti pareiškėjo bankui keliamo reikalavimo pagrįstumą, Lietuvos bankas vertins, ar: 1) mokėjimo operacijos laikytinos autorizuotomis; 2) bankas turi pareigą grąžinti ir (ar) kompensuoti pareiškėjui mokėjimo operacijų sumą; 3) bankas užtikrino banke laikomų pareiškėjo lėšų saugumą.

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.

1. Dėl mokėjimo operacijų autorizavimo

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).

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 mokėjimo paslaugų teikėjo sudaromoje bendrojoje mokėjimo paslaugų teikimo sutartyje (toliau – bendroji sutartis).

Banko mokėjimo paslaugų teikimo sąlygų (toliau – Sąlygos) 11.9 papunktyje nustatyta,

kad „mokėjimo operacija laikoma autorizuota tik tada, kai Klientas duoda sutikimą ją vykdyti. Šio sutikimo davimo forma ir tvarka nustatoma sutartyje. Klientas gali autorizuoti mokėjimo operaciją iki jos įvykdymo arba ją įvykdęs, jeigu taip susitarė Klientas ir Bankas. Jeigu pirmiau nurodyto sutikimo nėra, laikoma, kad mokėjimo operacija yra neautorizuota.“ Vadovaujantis Sąlygų 6.3.1 papunkčio, nurodančio, kokiais būdais banko klientas gali pateikti sutikimą atlikti operaciją, nuostatomis, „Klientas sutikimą atlikti mokėjimo operaciją gali pateikti Banko nustatyta arba Banko ir Kliento sutarta forma ir būdu. <...> Sutikimas dėl mokėjimo operacijų taip pat gali būti tvirtinamas naudojant Kliento atpažinimo priemones ir / ar kitais Bankui priimtinais būdais / priemonėmis. Atsiskaitant kortele, tam tikrais atvejais, kortelės turėtojas sutikimą atlikti mokėjimo operaciją taip pat gali patvirtinti pateikdamas kortelės duomenis ar nustatytu eiliškumu atlikdamas tam tikrus veiksmus (kortelės įdėjimas į tam skirtą vietą, kortelės priglaudimas prie specialiu ženklu pažymėto kortelių aptarnavimo skaitytuvo, konkrečios paslaugos ar prekės užsakymas), kurie jam siūlomi savitarnos ir kitose atsiskaitymo vietose. <...> Visais šiame punkte nurodytais būdais patvirtintas sutikimas atlikti mokėjimo operaciją ar dokumentai, laikomi patvirtintais Kliento ir / ar kortelės turėtojo (kortelės operacijų atveju) ir turinčiais tokią pat teisinę galią kaip ir Kliento ir / ar kortelės turėtojo (kortelės operacijų atveju) pasirašyti popieriniai dokumentai.“

Nagrinėjamo ginčo atveju, pareiškėjas savo mokėjimo kortelės personalizuotus saugumo duomenis panaudojo fiktyvioje – atsiradusioje paspaudus elektroniniu paštu gautą nuorodą, interneto svetainėje ir juos suvedė turėdamas tikslą įvykdyti 1,90 Eur mokėjimo operaciją atsiskaitant už pašto siuntos išlaidas. Tačiau pareiškėjas naudodamas savo mokėjimo priemonę neturėjo tikslo savo mokėjimo kortelę pridėti prie *Apple Pay* ir tokiu būdu iš savo sąskaitos banke įvykdyti 12 mokėjimo operacijų, kurių bendra suma - 2 263,95 Eur. Taigi, nagrinėjimo ginčo atveju, nors ir galima teigi, kad pareiškėjas mokėjimo priemonę naudojo pagal paskirtį – įvykdyti mokėjimo operaciją, tačiau taip pat galima teigti, kad pareiškėjas neišreiškė savo valios dėl 12 mokėjimo operacijų įvykdymo, kurios buvo įvykdytos iš pareiškėjo banko sąskaitos panaudojus *Apple Pay* mokėjimo patvirtinimo metodą.

Banko teigimu, mokėjimo operacijų įvykdymas buvo patvirtintas banko ir pareiškėjo sutartu būdu, t. y. pats pareiškėjas sukčių suklastotoje interneto svetainėje suvedė savo mokėjimo kortelės duomenis bei tretiesiems asmenims atskleidė SMS žinute gautą vienkartinį saugos kodą. Dėl šios priežasties mokėjimo operacijos laikytinos pareiškėjo autorizuotomis.

Lietuvos banko vertinimu, vien faktas, kad pareiškėjo mokėjimo kortelė buvo pridėta prie *Apple Pay* panaudojant mokėjimo kortelės duomenis ir SMS žinute pareiškėjui išsiųstą vienkartinį saugos kodą, neįrodo, kad mokėjimo operacijos iš tiesų atliktos gavus pareiškėjo sutikimą. Vadovaujantis Mokėjimų įstatymo nuostatomis, vien aplinkybė, kad mokėtojo mokėjimo paslaugų teikėjo vidaus sistemose užregistruotas mokėtojui išduotos mokėjimo priemonės, įskaitant jos personalizuotus saugumo duomenis, naudojimas, nebūtinai yra pakankamas įrodymas, kad mokėjimo priemone naudojosi ir (arba) mokėjimo operaciją autorizavo pats mokėtojas (Mokėjimų įstatymo 37 straipsnio 3 dalis).

Būtina atkreipti dėmesį ir į tai, kad, nustatytais duomenimis, mokėjimo operacijoms inicijuoti būtini duomenys buvo suvesti suklastotoje interneto svetainėje, kurioje pareiškėjui buvo rodoma informacija apie 1,90 Eur mokėjimo operaciją už pašto siuntos išlaidas, tačiau nebuvo rodoma informacija apie tai, kad pareiškėjo mokėjimo kortelė bus pridėta prie *Apple Pay* ir tokiu būdu bus įvykdyta ne viena 1,90 Eur mokėjimo operacija, o iš viso 12 mokėjimo operacijų.

Vadinasi, ginčo byloje esantys įrodymai, tarp jų ir pirmiau aptarti duomenys dėl mokėjimo operacijų inicijavimo ir įvykdymo aplinkybių, kurių nepaneigė banko paaiškinimai ir pateikti vidinės sistemos duomenys, kad mokėjimo kortelės pridėjimui prie *Apple Pay* panaudoti pareiškėjo mokėjimo kortelės duomenys ir vienkartinis saugos kodas, Lietuvos banko vertinimu, leidžia pagrįstai daryti išvadą, kad trečiųjų asmenų sukurtoje aplinkoje pareiškėjui apie prašymą atskleisti mokėjimo kortelės personalizuotus saugumo duomenis, būtinus mokėjimo kortelę pridėti prie *Apple Pay,* buvo rodoma tikrovės neatitinkanti informacija, kuri galėjo suklaidinti pareiškėją dėl prašomų atlikti veiksmų (atskleidžiamos konfidencialios informacijos) esmės ir pobūdžio. Vadinasi, duomenų, kad pareiškėjas žinojo, suprato ir išreiškė savo valią inicijuoti ir autorizuoti mokėjimo operacijas šalių sutarta tvarka, ginčo byloje nėra.

Atsižvelgiant į tai, Lietuvos banko nuomone, vertinti mokėjimo operacijas kaip autorizuotas – atliktas esant paties pareiškėjo sutikimui (kaip tai suprantama Mokėjimų įstatymo 29 straipsnio 1 dalies kontekste), nėra pagrindo, todėl Lietuvos bankas daro išvadą, kad mokėjimo operacijos laikytinos neautorizuotomis.

2. Dėl neautorizuotų mokėjimo operacijų pasekmių ir pareiškėjo 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 pareiškėjo mokėjimo kortelės duomenis bei kitus personalizuotus saugos duomenis tik todėl, kad pareiškėjas dėl savo didelio neatsargumo neįvykdė Mokėjimų įstatymo 34 straipsnyje nustatytų mokėtojo pareigų ir neužtikrino, kad, be pareiškėjo, turinčio teisę naudotis mokėjimo priemone, personalizuotais saugumo duomenimis negalėtų pasinaudoti kiti asmenys.

Tiek pareiškėjo, tiek banko paaiškinimai apie mokėjimo operacijų įvykdymo aplinkybes iš dalies sutampa – tiek bankas, tiek pareiškėjas teigia, kad tretieji asmenys pareiškėjo mokėjimo kortelės duomenis neteisėtai pasisavino kuomet pareiškėjas paspaudė trečiųjų asmenų jam atsiųstą aktyvią nuorodą. Tačiau pareiškėjo ir banko argumentai išsiskiria dėl SMS žinute banko išsiųsto vienkartinio saugos kodo perdavimo tretiesiems asmenims – pareiškėjas teigia savo mobiliojo telefono numeriu negavęs SMS žinutės su vienkartiniu saugos kodu ir nurodo, kad dėl banko sistemos spragų banko SMS žinutė su vienkartiniu saugos kodu galėjo patekti tiesiai pas trečiuosius asmenis. Bankas teigia, kad jo vidinių sistemų užfiksuoti duomenys įrodo, kad pareiškėjo mobiliojo telefono numeriu buvo išsiųsta SMS žinutė su vienkartiniu saugos kodu, o šis kodas buvo panaudotas mokėjimo kortelės duomenis pridedant prie *Apple Pay*.

Ginčo byloje nustatyta, kad pareiškėjas elektroniniu paštu iš trečiųjų asmenų gavo laišką neva iš *LP Express* su raginimu paspausi aktyvią nuorodą ir sumokėti 1,90 Eur už pašto siuntos išlaidas. Pareiškėjas paspaudęs jam pateiktą nuorodą neva *LP Express* puslapyje suvedė savo mokėjimo kortelės duomenis, kuriuos nusavino tretieji asmenys ir panaudojo pareiškėjo mokėjimo kortelę pridedant prie *Apple Pay.*

Banko pateiktais duomenimis, 2022 m. balandžio 19 d. 13:55 val. pareiškėjas savo mobiliojo telefono numeriu iš banko gavo SMS žinutę su tokiu pranešimo testu: „Įveskite kodą *duomenys neskelbiami* norėdami pridėti kortelę į skaitmeninę piniginę. Šis kodas galioja 30 minučių". Pareiškėjas neigia šį kodą gavęs ir atskleidęs tretiesiems asmenims, tačiau banko pateikti duomenys įrodo, kad vienkartinis saugos kodas buvo siųstas į pareiškėjo bankui nurodytą telefono numerį ir kad jis buvo panaudotas mokėjimo kortelei pridėti prie *Apple Pay.* Duomenų, kad pareiškėjo mobiliuoju telefonu galėjo naudotis ne pats pareiškėjas, ginčo byloje nėra. Vadinasi, niekas kitas be paties pareiškėjo vienkartinio saugos kodo duomenų negalėjo žinoti ir jų perduoti tretiesiems asmenims.

Pagal ginčo byloje pareiškėjo pateiktus paaiškinimus, spausdamas trečiųjų asmenų jam

atsiųstoje žinutėje pateiktą aktyvią nuorodą ir vesdamas savo kortelės duomenis jis tikėjosi inicijuoti 1,90 Eur mokėjimo operaciją už pašto siuntos išlaidas. Pareiškėjo teigimu, jis panašių laiškų dėl ateinančių siuntų gaudavo kasdien, todėl jam nekilo joks įtarimas, kad tai gali būti sukčiavimo ataka.

Teigdamas, kad pareiškėjo elgesys, dėl kurio jis prarado savo mokėjimo priemonę, turi didelio neatsargumo požymių, bankas remiasi tuo, kad pareiškėjas 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 pareiškėjo veiksmus, kuriais, kaip pats pareiškėjas pripažįsta, tretiesiems asmenims perdavė savo mokėjimo kortelės duomenis, turėdamas tikslą inicijuoti 1,90 Eur mokėjimo operaciją, pažymėtina, kad galima teigti, kad pareiškėjo mokėjimo kortelės duomenų naudojimo tikslas atitiko mokėjimo priemonės naudojimo paskirtį, dėl kurios ginčo šalys susitarė sutartyje.

Tačiau svarbu pažymėti, kad, banko pateiktais duomenimis, banko pareiškėjui 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. Pareiškėjas teigia, kad šios banko siųstos SMS žinutės jis nebuvo gavęs, nes ji dėl banko sistemos spragų galėjo patekti tiesiai tretiesiems asmenims. Visgi, ginčo byloje surinkti įrodymai šių pareiškėjo teiginių nepatvirtina, o priešingai patvirtina, kad bankas pareiškėjo mobiliojo telefono numeriu išsiuntė SMS žinutę su vienkartiniu saugos kodu ir šis kodas buvo panaudotas mokėjimo kortelę pridedant prie *Apple Pay.* Atsižvelgiant į tai, galima daryti išvadą, kad labiau tikėtina, kad pareiškėjas minėtą vienkartinį saugos kodą atskleidė tretiesiems asmenims.

Nagrinėjamo ginčo aplinkybių kontekste, galima vertinti, kad pareiškėjui turėjo sukelti įtarimų minėta SMS žinutėje banko pareiškėjui pateikta informacija, todėl pareiškėjas turėjo kritiškai vertinti savo tolimesnius veiksmus ir nuo jų susilaikyti, juolab, kad jis neketino mokėjimo kortelės pridėti prie *Apple Pay*, o ketino įvykdyti 1,90 Eur mokėjimo operaciją. Jeigu šio SMS žinute siųsto vienkartinio saugos kodo pareiškėjas nebūtų atskleidęs, mokėjimo kortelė nebūtų galėjusi būti pridėta prie *Apple Pay* ir mokėjimo operacijos nebūtų buvę įvykdytos. Tačiau pareiškėjas 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 patvirtinti 1,90 Eur mokėjimo operacijos įvykdymą ir toliau tęsė neatsargius veiksmus.

Lietuvos banko nuomone, jeigu pareiškėjas būtų buvęs pakankamai atidus ir kritiškas savo atliekamų veiksmų atžvilgiu, būtų pastebėjęs, kad jo prašoma atlikti veiksmus, kurie nėra susiję su 1,90 Eur mokėjimo operacijos įvykdymu, būtų galėjęs pastebėti trečiųjų asmenų neteisėtus veiksmus ir, labai tikėtina, būtų išvengęs neautorizuotų mokėjimo operacijų iš jo banko sąskaitos įvykdymo. Vis dėlto pareiškėjas elgėsi nerūpestingai ir toliau vykdė trečiųjų

asmenų jam pateiktus nurodymus.

Lietuvos banko vertinimu, pareiškėjo elgesys gali būti pripažintas kaip elgesys, iš esmės besiskiriantis nuo atsargaus elgesio reikalavimų, kuris galiausiai ir lėmė tai, kad pareiškėjas prarado savo mokėjimo priemonę, o tretieji asmenys įgijo galimybę pareiškėjo 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 pareiškėjas 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 pareiškėjo veiksmai, dėl kurių jis prarado mokėjimo priemonę, pasireiškė dideliu neatsargumu, tai galiausiai ir lėmė, kad buvo įvykdytos neautorizuotos mokėjimo operacijos iš pareiškėjo sąskaitos ir pareiškėjas 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 pareiškėjui taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, todėl pareiškėjo reikalavimas bankui grąžinti neautorizuotų mokėjimo operacijų lėšų sumą yra nepagrįstas ir atmestinas.

3. Dėl pareiškėjo banke laikomų lėšų saugumo

Kaip minėta pirmiau, nagrinėdamas ginčus Lietuvos bankas neatlieka patikrinimų tam, kad nustatytų, ar nebuvo pažeisti finansų įstaigų veiklai keliami teisės aktų reikalavimai. Lietuvos bankas remiasi ginčo šalių pateiktais konkrečiais įrodymais, kurių pagrindu priima sprendimą.

Vien aplinkybė, kad iš pareiškėjo sąskaitos buvo įvykdytos mokėjimo operacijos, kurių pareiškėjas teigia pats neinicijavęs, savaime nepagrindžia aplinkybės, kad banko taikytos klientų lėšų apsaugos priemonės buvo nepakankamos ir (ar) neatitinkančios teisės aktų reikalavimų ir būtent tai galėjo nulemti mokėjimo operacijų įvykdymą.

Duomenų, kad bankas būtų nevykdęs finansų rinką reglamentuojančių teisės aktų reikalavimų ir (ar) nesiėmęs priemonių užtikrinti savo klientų, įskaitant pareiškėjo, banke laikomų lėšų saugumo, nagrinėjant ginčą nenustatyta. Priešingai, iš byloje turimų duomenų matyti, kad bankas taikė saugesnio autentiškumo patvirtinimo procedūrą, t. y. užtikrino, kad prie pareiškėjo banko sąskaitos būtų jungiamasi tik naudojat pareiškėjui žinomus ir (ar) tik jo patvirtintus personalizuotus saugumo duomenis.

Remdamasi tuo, kas išdėstyta, ir vadovaudamasi 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