LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

SPRENDIMAS DĖL X.X. IR „PAYSERA LT", UAB, GINČO NAGRINĖJIMO

[Data] Nr. [Nr.]
Vilnius

Lietuvos bankas gavo X.X. (toliau – pareiškėjas) kreipimąsi, kuriuo prašoma išnagrinėti tarp pareiškėjo ir „Paysera LT", UAB, (toliau – bendrovė) kilusį ginčą.

N u s t a t y t a:

2021 m. lapkričio 4 d. prisijungus prie pareiškėjo paskyros bendrovėje iš pareiškėjo sąskaitos buvo atliktos penkios mokėjimo operacijos gavėjui Carmenui Cartai (Carmen Carta) (toliau – gavėjas): 12:45:47 val. 3 000 Eur; 12:46:14 val. 3 000 Eur; 12:47:34 val. 1 030 Eur; 12:56:13 val. 3 400 Eur; 13:05:01 val. 120 Eur (toliau – mokėjimo operacijos). Bendra mokėjimo operacijų suma – 10 550 Eur.

Pareiškėjas 2021 m. lapkričio 4 d. 13:14:46 val. telefonu kreipėsi į bendrovę ir pranešė, kad iš jo sąskaitos bendrovėje buvo atliktos penkios mokėjimo operacijos, kurių jis pats neinicijavo ir nedavė joms sutikimo. Bendrovė, gavusi pareiškėjo pranešimą, pradėjo tyrimą, kreipėsi į gavėjo finansų įstaigą dėl lėšų sugrąžinimo ir 2021 m. gruodžio 28 d. į pareiškėjo sąskaitą grąžino 3 953,81 Eur, tokią sumą pavyko sugrąžinti iš gavėjo finansų įstaigos.

2021 m. gruodžio 6 d. pareiškėjas kreipėsi į bendrovę prašydamas grąžinti jo neautorizuotų mokėjimo operacijų lėšas. Pareiškėjas savo pretenzijoje bendrovei paaiškino, kad 2021 m. lapkričio 4 d. 13 val. 02 min. į savo mobilųjį telefoną gavo elektroninį laišką apie sėkmingai pakeistą pareiškėjo paskyros slaptažodį, nors pareiškėjas slaptažodžio keitimo pats neinicijavo ir neatliko. Pareiškėjui ši žinutė sukėlė įtarimų, todėl jis prie savo paskyros jungėsi per bendrovės aplikaciją savo mobiliajame telefone, tačiau jam nepavyko prisijungti dėl autorizacijos klaidos. Pareiškėjas paaiškino, kad atnaujino paskyros slaptažodį, prisijungė prie savo paskyros per bendrovės mobiliąją aplikaciją savo telefone ir pastebėjo, kad iš jo sąskaitos bendrovėje atliktos penkios mokėjimo operacijos, kurių pareiškėjas pats neinicijavo ir nedavė joms sutikimo. Pareiškėjas paaiškino, kad „maždaug valandą prieš man gaunant žinutę apie mano neinicijuotą slaptažodžio keitimą buvau prisijungęs prie Paysera LT paskyros nešiojamu kompiuteriu ketindamas atlikti pavedimą į JAV. Šio veiksmo sėkmingai atlikti tuo metu man nepavyko, nes paskutiniuose žingsniuose atliekant pinigų pervedimo patvirtinimą naršyklės lange pasirodė užrašas, apie įvykusią autorizacijos veiksmo klaidą (tikslaus pranešimo teksto neįsidėmėjau), bet tai man jokių įtarimų nesukėlė, nes pamaniau, kad taip galėjo nutikti dėl prasto internetinio ryšio ir ketinau operaciją pakartoti šiek tiek vėliau." Pareiškėjas teigia, kad pasinaudoti nešiojamuoju kompiuteriu buvo priverstas dėl riboto mobiliosios aplikacijos funkcionalumo, ribojusio pareiškėjo galimybes atlikti pavedimą JAV doleriais iš pareiškėjo turimos sąskaitos bendrovėje. Kai mokėjimo operacijos buvo inicijuotos, pareiškėjas buvo Egipte. Pareiškėjas paaiškino, kad tik po to, kai bendrovė jo paprašė pateikti kompiuterio naršyklės išklotinę, paaiškėjo, kad pareiškėjas nežinomu būdu galėjo būti nukreiptas ne į tikrąjį bendrovės interneto puslapį: „Man nežinomu būdu ir metu aukščiau minėtų operacijų metu galėjau būti nukreiptas į ne Paysera LT priklausantį tinklapį, tačiau šio tinklo turinys (tiek vaizdinė, tiek tekstinė informacija) man tuo metu jokių įtarimų nesukėlė, nes buvo identiškas Paysera LT, kurį mačiau sėkmingai atliekant pinigų pervedimo operaciją dieną prieš tai (2021 m. lapkričio 3 d.). Taip pat čia matėsi visa informacija apie mano sąskaitas, bei anksčiau atliktas operacijas, operacijų šablonai ir pan." Pareiškėjas teigė, kad „naudojantis kompiuteriu į naršyklę nesuvedinėjau klaidingo, ne Paysera LT priklausančio tinklapio adreso, nes, kaip minėjau aukščiau, Paysera LT naudojausi diena prieš tai iš to pačio kompiuterio atlikdamas sėkmingą pinigų pervedimo operaciją į JAV esančio banko sąskaitą, o naršyklėje įprastai išlieka naršytų tinklapių istorinės nuorodos, kuriomis aš natūraliai ir įprastai pasinaudojau."

Pareiškėjo nuomone, neautorizuotos mokėjimo operacijos buvo įvykdytos dėl nepakankamų bendrovės IT sistemų saugos sprendimų ar jų nebuvimo.

Kaip ir minėta, bendrovei 2021 m. gruodžio 28 d. pavyko iš gavėjo finansų įstaigos sugrąžinti dalį mokėjimo operacijų lėšų, tačiau likusi dalis – 6 596,19 Eur, pareiškėjui nebuvo sugrąžinta. Bendrovei nesutikus pareiškėjui grąžinti likusios 6 596,19 Eur sumos, pareiškėjas kreipėsi į Lietuvos banką dėl vartojimo ginčo nagrinėjimo. Pareiškėjas Lietuvos bankui paaiškino, kad 2021 m. lapkričio 4 d., pareiškėjui naudojantis bendrovės paslaugomis ir bandant pervesti pinigines lėšas, buvo įsilaužta į pareiškėjo paskyrą ir iš jos atliktos pareiškėjo neautorizuotos mokėjimo operacijos. Kreipimesi į Lietuvos banką pareiškėjas plačiau mokėjimo operacijų vykdymo aplinkybių nedetalizavo, tačiau Lietuvos bankui telefonu teigė, kad visa tai detaliai išdėstė savo 2021 m. gruodžio 6 d. pretenzijoje bendrovei, taigi, pretenzijoje pateikta informacija Lietuvos bankas gali remtis nagrinėdamas šį ginčą. Pareiškėjas prašė rekomenduoti bendrovei grąžinti 6 596,19 Eur mokėjimo operacijų sumą.

Bendrovė Lietuvos bankui pateiktame atsiliepime paaiškino, kad pripažįsta, kad pareiškėjas galėjo tapti trečiųjų asmenų neteisėtų veiksmų auka, dėl to tretieji asmenys galėjo nusavinti pareiškėjo prisijungimo prie paskyros duomenis ir iš pareiškėjo sąskaitos be pareiškėjo žinios ir sutikimo įvykdyti pareiškėjo neautorizuotas mokėjimo operacijas. Bendrovė savo atsiliepime teigė identifikavusi, kad pareiškėjas dėl didelio neatsargumo pasidalijo savo prisijungimo duomenimis su galimai nusikalstamą veiką organizavusiais asmenimis ir taip prarado pinigines lėšas.

Atlikusi vidinį tyrimą, bendrovė nustatė, kad pagrindinis IP adresas, iš kurio įprastai prie bendrovės paskyros jungėsi pareiškėjas, yra *duomenys neskelbiami* (Lietuvos Respublika). Prie pareiškėjo paskyros buvo jungiamasi ir iš kitų neįprastų IP adresų: 2021 m. rugsėjo 24 d. 02:46:03 val. ir 02:48:13 val. iš IP adreso *duomenys neskelbiami* (Ispanijos Karalystė); 2021 m. lapkričio 3 d. 10:37:04 val. iš IP adreso *duomenys neskelbiami* (Egipto Arabų Respublikoje).

Bendrovė nustatė, kad 2021 m. lapkričio 3 d. 11:11:48 val. (Lietuvos laiku) buvo pakeistas pareiškėjo sąskaitos mėnesio limitas ir padidintas iki 15 000 Eur. Bendrovės teigimu, kadangi tokio pobūdžio pakeitimai siekiant apsaugoti pinigines lėšas nuo neteisėto piniginių lėšų pasisavinimo įsigalioja tik po 12 valandų, apie šį sąskaitos limito pakeitimą pareiškėjas buvo informuotas elektroninio pašto adresu. Pareiškėjas Lietuvos bankui telefonu patvirtino, kad pats inicijavo šį mėnesio limito savo sąskaitoje padidinimą.

2021 m. lapkričio 3 d. 11:55:52 val. (Lietuvos laiku) pareiškėjui buvo išsiųsta SMS žinutė bendrovės sistemoje pareiškėjo nurodytu telefono numeriu su unikaliu patvirtinimo kodu, skirtu slaptažodžio pakeitimui patvirtinti. 2021 m. lapkričio 3 d. 11:57:43 val., prisijungus prie bendrovės paskyros iš IP 41.33.56.98 adreso Egipto Arabų Respublikoje, buvo pakeistas pareiškėjo paskyros slaptažodis. 2021 m. lapkričio 3 d. 11:57:42 val. elektroninio pašto adresu pareiškėjas buvo informuotas apie sėkmingai pakeistą slaptažodį. Pareiškėjas Lietuvos bankui patvirtino, kad pats atliko šiuos veiksmus.

2021 m. lapkričio 4 d. 12:43:43 val. buvo užfiksuotas pirmasis prisijungimas prie pareiškėjo paskyros iš IP adreso *duomenys neskelbiami* Patikrinus šį IP adresą, buvo nustatyta, jog šiam prisijungimui buvo naudotas VPN, o tikroji prisijungimo šalis – Prancūzija, prisijungus buvo atlikti galimai paties pareiškėjo neinicijuoti piniginių lėšų pervedimai į gavėjo sąskaitą, o prisijungus iš IP adreso *duomenys neskelbiami*, buvo pakeistas pareiškėjo paskyros slaptažodis, kiti veiksmai pareiškėjo paskyroje buvo atlikti iš IP adreso *duomenys neskelbiami* Egipto Arabų Respublikoje.

Įvertinusi vidaus tyrimo metu surinktą informaciją, bendrovė padarė išvadą, kad 2021 m. lapkričio 4 d. pareiškėjas prie paskyros mėgino prisijungti *Google* naršyklėje rastu suklastotu bendrovės interneto svetainės adresu *www.paeyserra.com,* suklastotame bendrovės interneto puslapyje pareiškėjas suvedė savo prisijungimo prie bendrovės sistemos duomenis (elektroninio pašto adresą arba telefono numerį ir slaptažodį) ir taip savo prisijungimo duomenimis pasidalijo su galimai nusikalstamą veiką organizuojančiais asmenimis, o šie panaudojo prisijungimo duomenimis jungdamiesi prie tikrosios bendrovės paskyros. 2021 m. lapkričio 4 d. 12:55:52 val. (Lietuvos laiku) pareiškėjui buvo išsiųsta SMS žinutė pareiškėjo bendrovei nurodytu telefono numeriu su unikaliu vienkartiniu prisijungimo prie paskyros iš kito įrenginio patvirtinimo kodu, pareiškėjas gautą kodą suvedė suklastotame interneto puslapyje ir taip kodą sužinojo galimai nusikalstamą veiką organizuojantys asmenys (tretieji asmenys). Dėl šių pareiškėjo veiksmų tretiesiems asmenims buvo suteikta galimybė prisijungti prie pareiškėjo sąskaitos ir inicijuoti piniginių lėšų pervedimą gavėjui.

Bendrovės teigimu, jeigu pareiškėjas suklastotame bendrovės interneto puslapyje nebūtų

suvedęs savo prisijungimo duomenų bei į pareiškėjo mobilųjį telefoną SMS žinute gauto vienkartinio saugos kodo, kuriuo buvo patvirtintas prisijungimas prie pareiškėjo paskyros ir sąskaitos iš kito įrenginio, tretieji asmenys nebūtų galėję prisijungti prie pareiškėjo paskyros ir iš pareiškėjo sąskaitos inicijuoti mokėjimo operacijų. Bendrovė taip pat paaiškino, kad net jeigu pareiškėjas būdamas nepakankamai atidus ir neatkreipė dėmesio, kad suklastoto bendrovės interneto puslapio adresas akivaizdžiai skyrėsi nuo tikrojo, pareiškėjui turėjo sukelti įtarimų bendrovės SMS žinutė, kuria prašoma patvirtinti prisijungimą prie paskyros iš naujo įrenginio. Pareiškėjui įtarimų nesukėlė nei gauta SMS žinutė dėl prisijungimo iš neatpažinto įrenginio patvirtinimo, nei tai, kad, naudojantis tikruoju bendrovės interneto puslapiu, prisijungimo patvirtinimo vaizdas yra kitoks, tikrame bendrovės interneto puslapyje nėra prašoma įvesti SMS žinute gauto kodo. Bendrovė teigė, kad minėtos aplinkybės patvirtina, kad pareiškėjo elgesys ir veiksmai laikytini kaip labai neatsargūs.

Bendrovė teigė, kad, vadovaujantis bendrovės Bendrosios mokėjimo paslaugų sutarties privatiems klientams (toliau – Sutartis) 13.4 papunkčiu, pareiškėjas įsipareigojo „apsaugoti ir neatskleisti bet kokių pagal šią Sutartį jo paties sukurtų ar jam suteiktų slaptažodžių ar kitokių Mokėjimo priemonių personalizuotų saugumo požymių tretiesiems asmenims ir neleisti kitiems asmenims naudotis paslaugomis Kliento vardu. Jei Klientas nesilaikė šio įsipareigojimo ir (arba) galėjo, bet neužkirto tam kelio ir (arba) tokius veiksmus atliko tyčia ar dėl didelio savo neatsargumo, Klientas pilna apimtimi prisiima dėl to patirtus nuostolius bei įsipareigoja atlyginti kitų asmenų nuostolius, jei jie buvo patirti dėl Kliento nurodytų veiksmų ar neveikimo.“ Bendrovės nuomone, nagrinėjamo ginčo atveju turi būti taikoma Lietuvos Respublikos mokėjimų įstatymo 39 straipsnio 3 dalis ir visi nuostoliai dėl neautorizuotų mokėjimo operacijų turėtų tekti pareiškėjui, nes jis juos patyrė dėl didelio neatsargumo neįvykdęs Mokėjimų įstatymo 34 straipsnyje nustatytų pareigų. Bendrovė prašė pareiškėjo reikalavimą atmesti 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. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Pareiškėjo ir bendrovės ginčas kilo dėl bendrovės atsisakymo grąžinti pareiškėjui dalį pareiškėjo vardu bendrovėje atidarytoje sąskaitoje atliktų mokėjimo operacijų lėšų. Bendrą mokėjimo operacijų lėšų sumą sudaro 10 550 Eur, tačiau, ginčo byloje turimais duomenimis, bendrovė dalį (3 953,81 Eur) mokėjimo operacijų lėšų pareiškėjui grąžino, todėl nagrinėjamo ginčo atveju spręstina tik dėl bendrovės pareigos pareiškėjui grąžinti likusią 6 596,19 Eur sumą, kuri, kaip minėta, yra dalis pareiškėjo prašomos grąžinti mokėjimo operacijų sumos.

Pareiškėjas teigia neautorizavęs mokėjimo operacijų, jos atliktos be jo žinios ir sutikimo, todėl prašė bendrovės grąžinti ir likusią mokėjimo operacijų lėšų dalį. Bendrovė sutinka, kad mokėjimo operacijos galėjo būti inicijuotos ne paties pareiškėjo, o neteisėtai veikiančių trečiųjų asmenų. Bendrovė teigia, kad tretieji asmenys iš pareiškėjo galėjo pasisavinti prisijungimo prie pareiškėjo paskyros duomenis ir pareiškėjui SMS žinute į jo bendrovei nurodytą mobiliojo telefono numerį atsiųstą vienkartinį saugos kodą ir taip įgyti galimybę iš kito įrenginio bei IP adreso prisijungti prie pareiškėjo paskyros bendrovėje ir inicijuoti mokėjimo operacijas tik todėl, kad pareiškėjas dėl savo didelio aplaidumo neišsaugojo personalizuotų saugos duomenų. Pareiškėjas teigia, kad, jungdamasis prie sukčių suklastotos bendrovės interneto svetainės, nieko neįprasto nepastebėjo ir nemano, kad jo veiksmai buvo labai aplaidūs, taip pat teigia, kad bendrovės IT sistemose nėra įdiegtų saugiklių arba jie yra nepakankami, todėl tretieji asmenys turėjo galimybę neteisėtai pasisavinti pareiškėjo mokėjimo priemonę.

Tarp šalių nėra ginčo, kad mokėjimo operacijoms įvykdyti nebuvo duotas pareiškėjo sutikimas, t. y. mokėjimo operacijas tiek bendrovė, tiek pareiškėjas pripažįsta neautorizuotomis. Lietuvos bankui pateikti duomenys taip pat leidžia tvirtinti, kad mokėjimo operacijos galėjo būti įvykdytos ne paties pareiškėjo, o trečiųjų asmenų. Atsižvelgiant į tai, kad iš esmės abi ginčo šalys sutaria, kad mokėjimo operacijos galėjo būti inicijuotos be pareiškėjo žinios ir sutikimo, sprendime toliau nebus analizuojamos su mokėjimo operacijų autorizavimo vertinimu susijusios aplinkybės.

Nagrinėjamo ginčo atveju ginčo šalys iš esmės nesutaria dėl to, kam turėtų tekti atsakomybė už neautorizuotų mokėjimo operacijų įvykdymą: bendrovė teigia, kad atsakomybė

už visas neautorizuotas mokėjimo operacijas turėtų tekti pareiškėjui, nes mokėjimo priemonę pareiškėjas prarado dėl savo didelio aplaidumo, pareiškėjas teigia, kad, jungdamasis prie suklastotos bendrovės interneto svetainės, nebuvo labai aplaidus, nes vizualiai viskas atrodė taip pat, kaip ir jungiantis prie tikrosios bendrovės svetainės, todėl nieko neįprasto nepastebėjo. Pareiškėjo nuomone, bendrovė nėra įdiegusi pakankamo IT sistemų saugumo, dėl to tretieji asmenys turėjo galimybę įvykdyti sukčiavimo ataką ir pasisavinti iš pareiškėjo prisijungimo prie paskyros duomenis, tai ir lėmė neautorizuotų mokėjimo operacijų įvykdymą.

Teigdama, kad pareiškėjas dėl didelio aplaidumo tretiesiems asmenims atskleidė savo personalizuotus saugos duomenis, bendrovė remiasi tuo, kad pareiškėjas per *Google* paieškos sistemą jungdamasis prie bendrovės paskyros nepastebėjo, kad sukčių suklastotas bendrovės interneto svetainės adresas *www.paeyserra.com* akivaizdžiai skyrėsi nuo bendrovės tikrojo svetainės adreso *www.bank.paysera.com* ir kad sukčių suklastotoje bendrovės svetainėje suvedė SMS žinute gautą vienkartinį saugos kodą, skirtą prisijungimui prie pareiškėjo paskyros patvirtinti. Pareiškėjas teigia, kad prie suklastotos bendrovės interneto svetainės jungėsi URL laukelyje suvesdamas pirmąsias bendrovės pavadinimo raides. Paspaudęs pirmą pateiktą bendrovės interneto adreso nuorodą pareiškėjas pateko į suklastotą bendrovės interneto svetainę, suklastota bendrovės svetainė vizualiai atrodė tokia pati, todėl jungdamasis prie suklastotos bendrovės svetainės pareiškėjas nieko neįprasto nepastebėjo, o SMS žinute gautas vienkartis saugos kodas ir prašymas jį suvesti pareiškėjui nekėlė jokio įtarimo. Telefonu Lietuvos bankui pareiškėjas paaiškino, kad ir anksčiau ne vieną kartą prie savo paskyros jungėsi iš kitų įrenginių ir SMS žinute gaudavo vienkartinį saugos kodą, kurį ir suvesdavo norėdamas prisijungti prie bendrovės paskyros. Be to, pareiškėjas paaiškino, kad dieną prieš įvykdant neautorizuotas mokėjimo operacijas keitė savo prisijungimo prie paskyros slaptažodį ir suvedė SMS žinute atsiųstą vienkartinį saugos kodą, todėl ir vėliau, kai iš savo kompiuterio jungėsi, kaip vėliau paaiškėjo, prie suklastotos bendrovės svetainės, faktas, kad jo buvo prašoma suvesti SMS žinute gautą vienkartinį kodą, jam nesukėlė jokių įtarimų.

Siekiant išspręsti tarp bendrovės ir pareiškėjo kilusį ginčą, reikia įvertinti, ar pareiškėjo elgesys, dėl kurio tretiesiems asmenims buvo atskleisti prisijungimo prie pareiškėjo paskyros duomenys, laikytinas labai neatsargiu ar tik neatsargiu.

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.

Dėl neautorizuotų mokėjimo operacijų pasekmių ir pareiškėjo teisės į mokėjimo operacijų sumos 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.

Kaip ir minėta, bendrovė teigia, kad tretieji asmenys galėjo pasisavinti pareiškėjo prisijungimo prie paskyros duomenis ir SMS žinute į pareiškėjo mobiliojo telefono numerį atsiųstą vienkartinį saugos kodą, kuriuo prisijungimas prie pareiškėjo sąskaitos iš kito įrenginio buvo patvirtintas tik todėl, kad pareiškėjas dėl savo didelio neatsargumo neišsaugojo savo prisijungimo prie paskyros duomenų ir tretiesiems asmenims atskleidė SMS žinute gautą vienkartinį saugos kodą. Bendrovė teigia, kad pareiškėjas dėl savo didelio aplaidumo neįvykdė Mokėjimų įstatymo 34 straipsnyje nustatytos pareigos saugoti savo mokėjimo priemonę.

Kad būtų galima įvertinti, ar pareiškėjas iki mokėjimo operacijos įvykdymo galėjo pastebėti, kad mokėjimo priemonė buvo neteisėtai pasisavinta, svarbūs ne tik bendrovės pateikti sistemų išrašų duomenys apie mokėjimo operacijų įvykdymą, bet ir ginčo šalių paaiškinimai apie mokėjimo priemonės praradimo ir mokėjimo operacijų įvykdymo aplinkybes. Vertinant ginčo šalių pateiktus paaiškinimus apie mokėjimo operacijų atlikimo aplinkybes, matyti, kad iš esmės ginčo šalių paaiškinimai apie aplinkybes, kuriomis tretieji asmenys galėjo pasisavinti prisijungimo prie paskyros duomenis ir be pareiškėjo žinios ir sutikimo inicijuoti mokėjimo operacijas, sutampa. Taip pat ir bendrovės pateikti sistemų išrašai patvirtina pareiškėjo pateiktus paaiškinimus apie mokėjimo operacijų inicijavimo ir įvykdymo aplinkybes.

Ginčo byloje nustatyta, kad pareiškėjas prarado savo prisijungimo prie paskyros duomenis, kai prie savo paskyros jungėsi URL laukelyje vesdamas bendrovės pavadinimo pirmas kelias raides ir paspaudęs vieną iš jam iššokusių nuorodų pateko į netikrą bendrovės svetainę *www.paeyserra.com*, tada joje suvedė savo prisijungimo prie paskyros duomenis bei SMS žinute gautą vienkartinį saugos kodą. Teigdama, kad pareiškėjo elgesys turi didelio aplaidumo požymių, bendrovė iš esmės remiasi dviem aplinkybėmis: 1. pareiškėjas nepastebėjo, kad sukčių suklastotos bendrovės svetainės adresas *www.paeyserra.com* akivaizdžiai skiriasi nuo tikrojo bendrovės svetainės adreso *www.bank.paysera.com*; 2. tikroje bendrovės paskyroje bendrovė neprašo suvesti SMS žinute gauto vienkartinio saugos kodo.

Nagrinėjamo ginčo atveju yra svarbi aplinkybė, susijusi su prisijungimo prie bendrovės paskyros praktika, kad jeigu prie bendrovės paskyros jungiamasi iš įrenginio, iš kurio bendrovės paslaugų vartotojas jau buvo jungęsis anksčiau, SMS žinute vienkartinis saugos kodas nėra siunčiamas ir prašomas suvesti. Tam, kad prisijungtum prie savo paskyros ir sąskaitos bendrovėje, pakanka tik suvesti savo paskyros vardą ir slaptažodį. Jeigu prie bendrovės paskyros yra jungiamasi iš bendrovei nepažįstamo įrenginio, pati prisijungimo seka skiriasi nuo tos, kuri yra sukčių suklastotoje bendrovės interneto svetainėje. Sukčiai suklastotoje bendrovės paskyroje SMS žinute gautą vienkartinį saugos kodą prašo suvesti dar tik jungiantis prie bendrovės paskyros (suvedant prisijungimo vardą, slaptažodį), nors jungiantis prie tikrosios bendrovės paskyros SMS žinute gautas kodas prašomas suvesti tik vėliau, jau esant prisijungus prie paskyros, tačiau dar negalint ja naudotis.

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).

Nagrinėjamo ginčo byloje tarp šalių nėra ginčo dėl neautorizuotų mokėjimo operacijų įvykdymo aplinkybių, t. y. tiek pareiškėjo pateikti paaiškinimai apie neautorizuotų mokėjimo operacijų įvykdymo aplinkybes, tiek bendrovės surinkti įrodymai patvirtina, kad pareiškėjo neautorizuotos mokėjimo operacijos buvo inicijuotos pareiškėjui dėl neteisėtų trečiųjų asmenų veiksmų praradus savo mokėjimo priemonę, tai lėmė neautorizuotų mokėjimo operacijų įvykdymą. Ginčo byloje nustatytais duomenimis, tretieji asmenys neteisėtu būdu iš pareiškėjo pasisavino jo mokėjimo priemonę, pareiškėjui mėginant jungtis prie savo paskyros bendrovėje URL laukelyje vedant bendrovės pavadinimo pirmąsias raides bei paspaudus nuorodą į sukčių suklastotą bendrovės interneto puslapį *www.paeyserra.com* ir joje suvedus savo prisijungimo vardą, slaptažodį bei SMS žinute gautą vienkartinį saugos kodą, kuriuo ir buvo patvirtintas prisijungimas prie pareiškėjo paskyros iš kito įrenginio. Taigi, pareiškėjas URL laukelyje vesdamas bendrovės pavadinimą ir mėgindamas prisijungti prie savo paskyros bendrovėje nepastebėjo, kad nuorodos į bendrovės svetainės interneto adresą pavadinimas *www.paeyserra.com* skiriasi nuo nuorodos į tikrąjį bendrovės interneto svetainės adresą pavadinimo *www.bank.paysera.com*. Bendrovė teigia, kad sukčių suklastotas bendrovės interneto svetainės adresas *www.paeyserra.com* akivaizdžiai skyrėsi nuo tikrojo bendrovės svetainės adreso *www.bank.paysera.com*, todėl faktas, kad pareiškėjas to nepastebėjo, įrodo pareiškėjo didelį neatsargumą.

Vertinant, ar pareiškėjo elgesys, kai jis URL laukelyje vesdamas bedrovės pavadinimą ir taip mėgindamas jungtis prie savo paskyros bendrovėje nepastebėjo, kad nuoroda į bendrovės svetainės adresą, kurią jis paspaudė, skyrėsi nuo tikrojo bendrovės svetainės adreso, gali būti vertinamas kaip labai neatsargus pareiškėjo elgesys, t. y. toks elgesys, dėl kurio mokėjimo priemonės turėtojo veiksmai iš esmės skiriasi nuo atsargaus elgesio reikalavimų, pažymėtina, kad, Lietuvos banko nuomone, negalima būtų daryti išvados, kad sukčių suklastoto bendrovės interneto svetainės adreso pavadinimas *www.paeyserra.com* ir tikrojo bendrovės svetainės adreso pavadinimas *www.bank.paysera.com* yra akivaizdžiai besiskiriantys, dėl to vartotojui turėtų ir galėtų būti akivaizdu, kad jis jungiasi ne prie savo tikrosios paskyros bendrovėje. Abiejų nuorodų pavadinimuose nurodomas bendrovės pavadinimas skiriasi tik tuo, kad sukčių suklastoto bendrovės interneto svetainės adreso pavadinimo pradžioje nėra žodžio „bank" ir paties bendrovės pavadinimas nurodytas klaidingai, tačiau vizualiai labai panašiai. Be to, reikšminga yra ir aplinkybė, kad bendrovės paslaugų vartotojas prisijungti prie savo paskyros bendrovėje gali ir per bendrovės nuorodą *www.paysera.lt*, ir per bendrovės nuorodą *www.bank.paysera.com*. Nagrinėjamo ginčo atveju pareiškėjas kaip tik ir mėgino prie bendrovės paskyros prisijungti per bendrovės nuorodą *www.paysera.lt*, tačiau nepastebėjo, kad paspaudė sukčių suklastotą bendrovės nuorodą *www.paeyserra.com*. Todėl yra normalu, kad vartotojas prie bendrovės paskyros jungdamasis jo pasirinktu vienu iš būdų gali pagrįstai tikėtis, kad prisijungs prie savo tikrosios paskyros, ir nesitikėti, kad pateks į sukčių suklastotą netikrą bendrovės paskyrą, kuri vizualiai yra panaši į tikrąją. Kadangi sukčiavimo ataka yra gana gerai parengta, net ir pakankamai atidžiam vartotojui yra beveik neįmanoma pastebėti, kad, atlikdamas įprastinius veiksmus, jis patenka į sukčių suklastotą netikrą bendrovės svetainę, kuri, be kita ko, yra ir vizualiai labai panaši į tikrąją bendrovės svetainę, taip pat pastebėti, suprasti ar kitaip įtarti, kad tretieji asmenys neteisėtai pasisavina jo mokėjimo priemonę ir įgyja galimybę be jo žinios ir sutikimo iš jo sąskaitos vykdyti mokėjimo operacijas.

Taigi, atsižvelgiant į pirmiau minėtą informaciją, vertinant pareiškėjo elgesį, nebūtų galima teigti, kad pareiškėjas, nepastebėdamas, kad sukčių suklastotas bendrovės interneto svetainės adresas *www.paeyserra.com* skiriasi nuo tikrojo bendrovės svetainės adreso *www.bank.paysera.com*, buvo labai neatsargus, t. y. kad šis pareiškėjo elgesys buvo toks, dėl kurio pareiškėjo veiksmai iš esmės skyrėsi nuo atsargaus elgesio, ir pasireiškė dideliu pareiškėjo neatsargumu. Taigi, Lietuvos banko vertinimu, pareiškėjo elgesio, dėl kurio jis pararado savo mokėjimo priemonę, negalima būtų vertinti kaip labai neatsargaus.

Teigdama, kad pareiškėjas dėl savo didelio neatsargumo prarado mokėjimo priemonę ir tai lėmė neautorizuotų mokėjimo operacijų įvykdymą, bendrovė remiasi ir aplinkybe, kad pareiškėjas sukčių suklastotoje bendrovės svetainėje *www.paeyserra.com* suvedė ne tik savo prisijungimo vardą, slaptažodį, bet ir SMS žinute gautą vienkartinį saugos kodą, skirtą prisijungimui prie pareiškėjo paskyros iš kito įrenginio patvirtinti. Bendrovės teigimu, jungiantis prie tikrosios bendrovės paskyros iš kito įrenginio, bendrovė savo paskyroje neprašo suvesti SMS žinute gauto vienkartinio saugos kodo, todėl pareiškėjui turėjo kilti įtarimas, kodėl jo prašoma SMS žinute gautą vienkartinį saugos kodą suvesti bendrovės paskyroje. Bendrovės

teigimu, pareiškėjas turėjo nesielgti labai neatsargiai ir bendrovės svetainėje nevesti SMS žinute gauto saugos kodo. Šiame kontekste paminėtina, kad, jungiantis prie sukčių suklastotos bendrovės paskyros, tiek prisijungimo vardą ir slaptažodį, tiek SMS žinute gautą saugos kodą yra prašoma suvesti jau atliekant pirmuosius žingsnius, o jungiantis prie tikrosios bendrovės paskyros iš kito įrenginio pirmiausia prašoma suvesti prisijungimo vardą ir slaptažodį ir tik vėliau, juos suvedus bei patekus į bendrovės paskyrą (tačiau dar negalint ja naudotis), yra prašoma papildomai autentifikuotis (patvirtinti prisijungimą per mobiliąją programėlę arba SMS žinute), jeigu jungiamasi iš kito įrenginio.

Vertinant bendrovės argumentą, kad pareiškėjui turėjo kilti įtarimas, kodėl jo prašoma SMS žinute gautą vienkartinį saugos kodą suvesti bendrovės paskyroje, nors, jungiantis prie tikrosios bendrovės paskyros iš kito įrenginio, bendrovė savo paskyroje neprašo suvesti SMS žinute gauto vienkartinio saugos kodo, svarbu tai, kad pareiškėjas prie sukčių suklastotos bendrovės svetainės *www.paeyserra.com* jungėsi iš įrenginio (kompiuterio), kuris bendrovės sistemoms jau buvo pažįstamas, nes pareiškėjas iš jo jau buvo jungęsis ir anksčiau. Kaip minėta, tokiu atveju jungiantis prie bendrovės paskyros papildomai autentifikuotis (patvirtinti prisijungimą per mobiliąją programėlę arba SMS žinute) nėra prašoma, o kad patektum į savo paskyrą, pakanka tik suvesti savo prisijungimo vardą bei slaptažodį. Taigi, kadangi pareiškėjas prie savo paskyros mėgino jungtis iš savo įrenginio, iš kurio jis buvo jungęsis jau ir anksčiau, jis galėjo tikėtis, kad tik suvedęs savo prisijungimo vardą bei slaptažodį pateks į savo paskyrą. Pareiškėjas negalėjo tikėtis, kad jo bus prašoma papildomai autentifikuotis suvedant SMS žinute gautą vienkartinį saugos kodą. Pareiškėjas galėjo tikėtis, kad prie savo paskyros prisijungs atlikęs pirmąjį veiksmą – suvedęs prisijungimo vardą ir slaptažodį. Tačiau pareiškėjo dar papildomai buvo prašoma prisijungimą prie paskyros patvirtinti SMS žinute gautu vienkartiniu saugos kodu, nes prie tikrosios pareiškėjo paskyros bendrovėje jungėsi tretieji asmenys, kurie pasisavino iš pareiškėjo prisijungimo prie paskyros duomenis.

Taigi, įvertinus pirmiau minėtas aplinkybes, galima teigti, kad pareiškėjo veiksmų, kuriuos ji anksčiau turėdavo atlikti norėdamas prisijungti prie bendrovės paskyros iš bendrovei jau pažįstamo įrenginio, seka ir veiksmų, kuriuos pareiškėjo buvo prašoma atlikti sukčių suklastotoje bendrovės aplinkoje, seka buvo labai panašios. Vienintelis skirtumas, kuris turėjo sukelti pareiškėjui įtarimą, buvo tas, kad jo buvo prašoma sukčių suklastotoje bendrovės aplinkoje suvesti SMS žinute gautą vienkartinį saugos kodą, kuriuo patvirtinamas prisijungimas prie paskyros iš kito įrenginio.

Pareiškėjas Lietuvos bankui teigė, kad SMS žinute gauto vienkartinio saugos kodo suvedimas, skirtas pareiškėjo prisijungimui prie savo paskyros iš kito įrenginio patvirtinti, nesukėlė jam jokių įtarimų, nes jis prie savo paskyros jungdavosi iš kitų įrenginių ir tuomet jis gaudavo SMS žinute vienkartinį saugos kodą, kurį ir suvesdavo. Be to, pareiškėjas teigė, kad dieną prieš jis keitė savo prisijungimo prie paskyros slaptažodį ir tokiam veiksmui patvirtinti jam taip pat jo telefonu buvo atsiųsta SMS žinutė, kurią jis suvedė tam, kad pakeistų prisijungimo prie savo paskyros slaptažodį. Todėl pareiškėjas manė, kad ir šį kartą SMS žinutė jam buvo atsiųsta tam, kad galėtų patvirtinti prisijungimą prie paskyros. Taigi, pareiškėjui nekilo jokių įtarimų, kad jis galėjo tapti trečiųjų asmenų neteisėtų veiksmų auka. Lietuvos bankui pateikti duomenys patvirtina šį pareiškėjo teiginį, t. y. iš pateiktų duomenų matyti, kad pareiškėjas prie savo paskyros bendrovėje jungdavosi iš kitų įrenginių ir iš skirtingose valstybėse registruotų IP adresų. Taip pat Lietuvos bankui pateikti duomenys patvirtina ir tai, kad pareiškėjas keitė savo prisijungimo prie paskyros slaptažodį ir tada iš bendrovės SMS žinute gavo vienkartinį saugos kodą. Taigi, remiantis pirmiau minėtomis aplinkybėmis, galima teigti, kad pareiškėjas suprato SMS žinute gauto vienkartinio saugos kodo paskirtį – patvirtinti prisijungimą prie savo paskyros, ir manė, kad suvesdamas SMS žinute gautą vienkartinį saugos kodą jungiasi prie savo paskyros bendrovėje, tačiau nepastebėjo, kad jungiasi prie sukčių suklastotos bendrovės interneto paskyros.

Vertinant pareiškėjo elgesio neatsargumo laipsnį, svarbu tai, kad bendrovės Bendrųjų mokėjimo paslaugų teikimo sąlygų privatiems klientams (toliau – Sąlygos) 5.1 papunktyje pareiškėjas ir bendrovė buvo sutarę dėl tokios sąskaitos valdymo tvarkos: „Klientas Paysera Sąskaitą gali valdyti internetu, prisijungęs prie savo Paskyros savo prisijungimo vardu ir Slaptažodžiu bei atlikęs papildomo prisijungimo (saugesnio autentiškumo patvirtinimo) procedūrą.“ Tokia šios Sąlygų nuostatos formuluotės leidžia teigti, kad vartotojas gali manyti, kad papildoma autentifikavimo procedūra yra įprastinis veiksmas, kurį vartotojas atlieka siekdamas internetu valdyti savo sąskaitą bendrovėje. Tai, kad siekiant valdyti savo sąskaitą ne visuomet gali reikėti papildomai autentifikuotis ir (arba) kad tai priklauso nuo to, iš kokio

įrenginio jungiamasi, iš minėtos Sąlygų nuostatos nėra aišku. Nagrinėjamo ginčo atveju taip pat galima vertinti, kad yra normalu, kad pareiškėjas, vesdamas SMS žinute gautą vienkartinį saugos kodą, galėjo pagrįstai manyti, kad su bendrove sutartu būdu jungiasi prie savo paskyros bendrovėje.

Svarbu pažymėti, kad pareiškėjas tapo gerai parengtos sukčių atakos auka ir, netgi prie savo paskyros bendrovėje mėgindamas jungtis URL laukelyje vesdamas bendrovės pavadinimą, vis tiek pateko į sukčių suklastotą bendrovės interneto svetainę. Kaip ir minėta, prie paskyros bendrovėje galima prisijungti ne tik per nurodą *www.bank.paysera.com*, bet ir per *www.paysera.lt*. Taigi, netgi ir tada, kai jungiasi URL laukelyje suvesdamas bendrovės pavadinimą, vartotojas nėra apsaugotas nuo to, kad nepateks į sukčių suklastotą bendrovės interneto svetainę, kuri, be kita ko, ir vizualiai yra labai panaši į tikrąją bendrovės svetainę. Taigi, įvertinus faktą, kad prie savo paskyros bendrovėje vartotojas gali prisijungti itin lengvai ir paprastai, rizika tapti trečiųjų asmenų neteisėtų veiksmų auka ir dėl to patirti nuostolių smarkiai padidėja, įvertinus faktą, kad nagrinėjamo ginčo atveju trečiųjų asmenų neteisėti veiksmai dėl gerai parengtos sukčiavimo atakos net ir pakankamai atsargiam vartotojui, objektyviai vertinant, yra sunkiai pastebimi, galima teigti, kad mokėjimo paslaugų teikėjai, be kitų mokėjimo operacijų įvykdymo saugumą užtikrinančių priemonių, turėtų imtis aktyvių veiksmų, kad jų klientai būtų laiku, tinkamai ir aiškiai informuojami apie visas galimas (žinomas) rizikas, susijusias su mokėjimo priemonės paradimu dėl neteisėtų trečiųjų asmenų veiksmų, ypač bendrovei turint informaciją apie prieš bendrovės klientus jau surengtas panašaus pobūdžio sukčių atakas. Nagrinėjamo ginčo atveju bendrovė nepateikė informacijos, kad savo klientus, įskaitant ir pareiškėją, būtų informavusi, kad bendrovė savo svetainėje neprašo papildomai suvesti SMS žinute gauto vienkartinio saugos kodo, kuriuo patvirtinamas prisijungimas prie bendrovės sąskaitos iš kito įrenginio, arba kad būtų atkreipusi klientų dėmesį į tai, kad ne visais atvejais bendrovė prašo papildomai autentifikuotis (pvz., jeigu jungiamasi iš bendrovei pažįstamo įrenginio). Lietuvos banko nuomone, bendrovė, gana ilgą laiko tarpą turėdama informaciją apie prieš jos klientus vykstančias tapačias sukčių atakas, turėtų imtis aktyvesnių veiksmų, siekdama apsaugoti savo paslaugų vartotojus nuo bendrovei jau žinomų tapačių sukčiavimo atakų. Vertinant bendrovės atsakomybę dėl to, kad bendrovė nesiėmė pakankamų veiksmų, kad jos klientai būtų geriau informuoti apie galimas rizikas dėl neteisėtų trečiųjų asmenų veiksmų prarasti savo mokėjimo priemonę, atkreiptinas dėmesys į Mokėjimų įstatymo 39 straipsnio 2 dalies 2 punkto nuostatą, kurioje teigiama, kad mokėtojas neturi patirti jokių nuostolių, jeigu nuostoliai yra patirti dėl mokėjimo paslaugų teikėjo, jo darbuotojo, tarpininko, filialo ar asmenų, kuriems perduotas veiklos funkcijų vykdymas, veiksmų ar neveikimo. Yra akivaizdu, kad vartotojas prie savo paskyros bendrovėje gali prisijungti itin paprastai, iš esmės per vieną žingsnį, todėl, i savo klientams siūlydama tokį paprastą būdą prisijungti prie savo paskyros ir ją valdyti, bendrovė turėtų dėti daug daugiau pastangų, siekdama informuoti savo klientus apie rizikas, su kuriomis jie gali susidurti, arba įdiegti papildomus saugiklius.

Atsižvelgiant į pirmiau nurodytas aplinkybes, negalima teigti, kad pareiškėjo elgesys, dėl kurio jis prarado savo mokėjimo priemonę, gali būti pripažįstamas kaip elgesys, pasireiškęs neprotingumu ar išskirtiniu rūpestingumo nebuvimu. Lietuvos banko vertinimu, sukčių suklastota bendrovės paskyra iš esmės ir akivaizdžiai nesiskyrė nuo tikrosios bendrovės paskyros, pareiškėjo atliekamų veiksmų seka jungiantis prie suklastotos bendrovės paskyros ir jungiantis prie tikrosios bendrovės paskyros iš to paties įrenginio iš esmės nesiskyrė, priešingai, buvo panaši, skyrėsi tik tuo, kad bendrovės tikroje svetainėje nėra prašoma suvesti SMS žinute gauto vienkartinio saugos kodo, o pačios SMS žinutės suvedimas su saugos kodu į sukčių suklastotą bendrovės interneto svetainę pareiškėjui galėjo atrodyti kaip įprastai atliekamas veiksmas, kurį pareiškėjas atlikdavo jungdamasis prie savo paskyros. Lietuvos banko nuomone, įvertinus pirmiau išdėstytas ginčo byloje nustatytas aplinkybes ir padarytas išvadas, galima teigti, kad pareiškėjas iki mokėjimo operacijos įvykdymo negalėjo pastebėti, kad jo mokėjimo priemonę pasisavino tretieji asmenys. Mokėjimų įstatymo 39 straipsnio 2 dalyje nustatyta, kad 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).

Vertinant Mokėjimų įstatymo nuostatas, reglamentuojančias atsakomybės už neautorizuotų mokėjimo operacijų įvykdymą pasiskirstymą, tam, kad bendrovė būtų atleista nuo pareigos grąžinti neautorizuotų mokėjimo operacijų lėšas, turėtų būti nustatytas pareiškėjo sukčiavimas arba didelis neatsargumas. Kaip ir buvo minėta, Lietuvos banko nuomone,

nagrinėjamo ginčo atveju pareiškėjo elgesys, dėl kurio jis prarado savo mokėjimo priemonę, negali būti laikomas labai neatsargiu, o apie galimą pareiškėjo sukčiavimą ar kitokį nesąžiningą veikimą ginčo byloje duomenų nėra. Įvertinus pirmiau išdėstytą informaciją, konstatuotina, kad pagrindo pareiškėjui taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį nėra. Kitų aplinkybių, kurios leistų pagrįstai manyti, kad pareiškėjui turėtų tekti visi su neautorizuotomis mokėjimo operacijomis susiję nuostoliai, ginčo byloje taip pat nenustatyta, todėl, Lietuvos banko vertinimu, pareiškėjo reikalavimas bendrovei grąžinti ir likusią dalį neautorizuotų mokėjimo operacijų lėšų sumos yra pagrįstas, todėl tenkintinas.

Remdamasis tuo, kas išdėstyta, ir vadovaudamasis Vartotojų teisių apsaugos įstatymo 27 straipsnio 1 dalies 1 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 59.1 papunkčiu, n u s p r e n d ž i u:

1. Tenkinti pareiškėjo X.X. reikalavimą ir rekomenduoti bendrovei grąžinti pareiškėjui 6 596,19 Eur.

2. Įpareigoti bendrovę 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