LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

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

2021-11-24 Nr. 429-435
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. rugpjūčio 4 d. 9:04:47 val. prisijungus prie pareiškėjo paskyros bendrovėje iš pareiškėjo sąskaitos buvo inicijuota 470 Eur mokėjimo operacija gavėjui Jean'ui Marie Plumain'ui (Jean Marie Plumain) (toliau – mokėjimo operacija).

2021 m. rugpjūčio 4 d. 9:30 val. pareiškėjas telefonu kreipėsi į bendrovę ir paprašė sustabdyti mokėjimo operaciją, nes iš jo sąskaitos įvykdytos mokėjimo operacijos jis pats neinicijavo. Bendrovė 2021 m. rugpjūčio 4 d. 09:49 val. apribojo pareiškėjo sąskaitą ir tą pačią dieną išsiuntė SWIFT pranešimą gavėjo bankui dėl galimai neautorizuotos mokėjimo operacijos lėšų grąžinimo.

2021 m. rugpjūčio 4 d. 11:02 val. bendrovė pareiškėjui išsiuntė užklausą dėl papildomos informacijos, susijusios su mokėjimo operacijos atlikimo aplinkybėmis, pateikimo. Bendrovė pareiškėjo paprašė pateikti informaciją, kokiu būdu atliekant mokėjimo operaciją pareiškėjas jungėsi prie bendrovės paskyros, pateikti savo naršyklės istoriją bei nurodyti, ar buvo sulaukęs skambučių iš asmenų, prisistatančių banko ar kitos finansinės institucijos atstovais. Taip pat paprašė pateikti informaciją, ar pareiškėjas nebuvo atskleidęs tretiesiems asmenims savo asmens duomenų ir prisijungimo prie paskyros duomenų.

Pareiškėjas 2021 m. rugpjūčio 4 d. atsakydamas bendrovei į užduotus klausimus teigė, kad prie bendrovės paskyros visada jungėsi per bendrovės aplikaciją savo mobiliajame telefone, skambučių iš asmenų, prisistatančių banko ar kitos finansinės institucijos atstovais, nebuvo sulaukęs, taip pat nebuvo atskleidęs ir savo prisijungimo prie paskyros duomenų tretiesiems asmenims.

Bendrovė atlikusi tyrimą nustatė, kad prie pareiškėjo paskyros buvo prisijungta iš kito įrenginio, o prisijungimas buvo patvirtintas saugesnio autentiškumo patvirtinimo procedūra. Bendrovė pareiškėjui pateikė atsakymą, kad negalės jam sugrąžinti mokėjimo operacijos lėšų.

2021 m. rugpjūčio 17 d. pareiškėjas su pretenzija kreipėsi į bendrovę nurodydamas, kad jam nežinant neteisėtai buvo prisijungta prie jo asmeninės sąskaitos bendrovėje. Pareiškėjas pabrėžė, kad prie savo sąskaitos prisijungti gali tik jis ir kad prisijungimo prie paskyros duomenų tretiesiems asmenims jis niekada nebuvo suteikęs. Pareiškėjas paaiškino, kad mokėjimo operacijos jis asmeniškai neatliko ir jokiomis priemonėmis jos nepatvirtino. Pareiškėjas teigė, kad bendrovė neapsaugojo jo lėšų bendrovės sąskaitoje, todėl turi grąžinti jo neautorizuotos mokėjimo operacijos lėšas – 470 Eur.

2021 m. rugpjūčio 18 d. bendrovė pareiškėjui pateiktame atsakyme į jo 2021 m. rugpjūčio 17 d. pretenziją teigė, kad nesutinka tenkinti pareiškėjo reikalavimo grąžinti mokėjimo operacijos lėšas, ir nurodė pareiškėjui kreiptis į teisėsaugos institucijas. Taip pat bendrovė paaiškino, kad, bendrovės turimais duomenimis, dėl nusikalstamu būdu organizuotos atakos, kurios metu buvo panaudotas suklastotas bendrovės puslapis *www.paeysera.com*, nukentėjo dalis bendrovės klientų: „Nukentėjusieji mėgindami prisijungti prie savo Paysera paskyros ir nebūdami pakankamai apdairūs jungėsi ne prie Paysera sistemos ir kliento paskyros, o prie suklastoto URL arba bendravo su neteisėtai Payseros atstovais prisistačiusiais asmenimis telefonu. Dėl tokio neatsargumo klientų prisijungimo prie Paysera paskyros duomenys tapo žinomi tretiesiems asmenims, kurie pasinaudodami šiais duomenimis iš nukentėjusių klientų sąskaitų atliko įvairaus dydžio pervedimus į sąskaitas, esančias kitose

finansų įstaigose, registruotose kitose valstybėse.“

Pareiškėjas nesutiko su bendrovės atsakymu, todėl kreipėsi į Lietuvos banką dėl vartojimo ginčo nagrinėjimo. Pareiškėjas paaiškino, kad jo vardu bendrovėje buvo atidarytos jo asmeninė sąskaita bei sąskaita, priklausanti juridiniam asmeniui *duomenys neskelbiami*, kuriai pareiškėjas atstovauja kaip vadovas. Pareiškėjas teigė, kad 2021 m. rugpjūčio 4 d., jam nežinant, neteisėtai buvo prisijungta prie jo asmeninės sąskaitos bei jo atstovaujamos įmonės *duomenys neskelbiami* sąskaitos ir be jo sutikimo įvykdytos mokėjimo operacijos, kurioms pareiškėjas nedavė sutikimo. Pareiškėjas pabrėžė, kad prie savo sąskaitos prisijungti gali tik jis pats pareiškėjas, be to, prisijungimo prie bendrovėje turimos savo paskyros duomenų tretiesiems asmenims nebuvo suteikęs.

Pareiškėjas paaiškino, kad bendrovė apie neteisėtus prisijungimus prie pareiškėjo paskyros ir pinigų iš sąskaitos vagystę buvo informuota 2021 m. rugpjūčio 4 d. 09:30 val. telefonu, pareiškėjui savo bendrovės mobiliojoje programėlėje pastebėjus, kad yra vykdomos jo nepatvirtintos finansinės operacijos. Pareiškėjas teigė, kad, jam pranešus apie pastebėtas vykdomas jo nepatvirtintas mokėjimo operacijas ir lėšų iš jo sąskaitos vagystę, bendrovės darbuotojai inicijavo mokėjimo operacijos atšaukimą ir už šią paslaugą, pareiškėjo iš anksto jo neinformavę, pritaikė po 10 Eur komisinį mokestį už vienos operacijos atšaukimą. Pareiškėjas prašė rekomenduoti bendrovei grąžinti jo neautorizuotos mokėjimo operacijos lėšas bei iš pareiškėjo sąskaitos nurašytą 10 Eur komisinį mokestį už mokėjimo operacijos atšaukimą.

Bendrovė Lietuvos bankui pateiktame atsiliepime paaiškino, kad patikrinusi pareiškėjo prisijungimų prie jo sąskaitos duomenis nustatė, kad, nepaisant to, kad pareiškėjas teigė, jog pats nesijungė prie savo paskyros bendrovėje naudodamasis netikru bendrovės puslapio adresu *www.paeysera.com* ir neatskleidė tretiesiems asmenims savo prisijungimo prie paskyros duomenų bei vienkartinio autentiškumą patvirtinančio kodo, bendrovės surinkti duomenys rodo, kad mokėjimo operacija buvo autorizuota remiantis saugesnio autentiškumo patvirtinimo procedūra.

Bendrovės turimais duomenimis, 2021 m. rugpjūčio 4 d. 08:14:47 val., prieš atliekant ginčijamą mokėjimo operaciją (kuri atlikta 2021 m. rugpjūčio 4 d. 9:04:47 val.), prie pareiškėjo sąskaitos buvo prisijungta iš IP adreso *duomenys neskelbiami*, registruoto Prancūzijoje. Būtent iš šio IP adreso ir buvo inicijuota mokėjimo operacija. Bendrovė nustatė, kad prisijungimas prie pareiškėjo paskyros ir kartu sąskaitos iš IP adreso, registruoto Prancūzijoje, buvo patvirtintas saugesnio autentiškumo patvirtinimo procedūra – prisijungimas buvo patvirtintas pareiškėjo mobiliuoju telefonu Nr. *duomenys neskelbiami* išsiųstu unikaliu vienkartiniu saugos kodu – *duomenys neskelbiami*. Bendrovės teigimu, šis kodas buvo panaudotas prijungiant papildomą mobiliojo telefono įrenginį prie pareiškėjo paskyros. Bendrovės nuomone, papildomas mobiliojo telefono įrenginys prie pareiškėjo paskyros buvo prijungtas trečiųjų asmenų, kurie ir sukūrė *www.paeysera.com* svetainę. Bendrovė teigė, kad iš turimų bendrovės sistemų išrašų matyti, kad, pareiškėjui neatskleidus į jo asmeninį mobilųjį telefoną gauto unikalaus vienkartinio kodo, saugesnio autentiškumo patvirtinimo procedūra nebūtų buvusi atlikta, o nusikalstamą veiklą vykdantys asmenys nebūtų galėję prisijungti prie pareiškėjo sąskaitos bendrovėje ir vykdyti neribotą kiekį mokėjimo operacijų. Bendrovė akcentavo, kad tam, kad tretieji asmenys galėtų prisijungti prie pareiškėjo paskyros ir iš jos inicijuoti mokėjimo operacijas, jiems turėjo būti žinomi pareiškėjo prisijungimo prie paskyros duomenys ir vienkartinis saugos kodas, kuris pareiškėjui buvo išsiųstas SMS žinute jo telefono numeriu.

Bendrovė pažymėjo, kad situacijos, į kurią dėl galimai neteisėtų trečiųjų asmenų veiksmų pateko pareiškėjas, faktinės aplinkybės, veiksmų seka bei jų išsidėstymas laike yra labai panašūs į bendrovei žinomą galimai nusikalstamu būdu organizuotą kibernetinę ataką. Bendrovės turimais duomenimis, nusikalstamu būdu buvo organizuota kibernetinė ataka, kai buvo panaudotas suklastotas adresas www.paeysera.com ir imituotas bendrovės interneto puslapis. Asmenys, mėgindami prisijungti prie savo paskyros bendrovėje, nebūdami pakankamai apdairūs, jungėsi ne prie bendrovės sistemos ir kliento paskyros, o prie sukčių suklastotos bendrovės svetainės. Dėl tokio neatsargumo klientų prisijungimo prie bendrovės paskyros duomenys tapo žinomi tretiesiems asmenims, kurie pasinaudodami šiais duomenimis iš klientų sąskaitų atliko įvairaus dydžio pervedimus į sąskaitas, esančias kitose finansų įstaigose, registruotose kitose valstybėse.

Bendrovės turimais duomenimis, pareiškėjo mokėjimo operacija galėjo būti autorizuota tokia seka:

1. Pareiškėjas spaudė reklaminę nuorodą *Google* sistemoje į netikrą bendrovės puslapį *www.paeysera.com* ir joje suvedė savo prisijungimo duomenis (el. pašto adresą, tel. numerį ir

prisijungimo slaptažodį) bei SMS žinute į savo telefono numerį gautą vienkartinį saugos kodą. Bendrovė atkreipė dėmesį, kad pareiškėjas turėjo pastebėti, kad suklastotos bendrovės svetainės adresas skiriasi nuo to, kuris yra bendrovės – *www.bank.paysera.com*.

2. Kadangi netikras bendrovės puslapis yra skirtas prisijungimo prie paskyros duomenims surinkti, sukčiai gautus duomenis nusavino, suvedė į savo mobiliajame telefone sukurtą bendrovės programėlę ir tokiu būdu per savo mobilųjį telefoną prisijungė prie pareiškėjo sąskaitos.

3. Tikėtina, kad, įvedus teisingą slaptažodį, netikras bendrovės puslapis automatiškai prijungiamas prie mobiliosios aplikacijos naujame įrenginyje, o kadangi nusikalstamą veiklą vykdantys asmenys neturi reikiamo autentiškumą patvirtinančio vienkartinio kodo, jie paprašė pareiškėjo suklastotoje svetainėje įvesti vienkartinį kodą, kurį SMS žinute bendrovė pareiškėjui išsiuntė į jo mobilųjį telefoną. Bendrovė pažymėjo, kad jeigu naudojamasi tikra bendrovės svetaine *www.bank.paysera.com*, joje neprašoma įvesti SMS žinute gauto kodo. Bendrovės teigimu, šis faktas turėjo pareiškėjui sukelti įtarimų.

4. Pareiškėjas SMS žinute gautą unikalų vienkartinį kodą (pareiškėjas jį gavo 2021 m. rugpjūčio 4 d. 08:14:11 val.) suvedė suklastotame bendrovės puslapyje, suvestą kodą sužinojo tretieji asmenys, jį suvedė savo mobiliajame įrenginyje ir sėkmingai prisijungė prie pareiškėjo sąskaitos (tai patvirtina sėkmingas prisijungimas 2021 m. rugpjūčio 4 d. 08:14:47 val. iš IP adreso Nr. *duomenys neskelbiami* Prancūzijoje).

5. Pareiškėjas, suvedęs SMS žinute gautą kodą į suklastotą bendrovės svetainę, gavo pranešimą apie sistemos klaidą arba kitokį pranešimą ir, tikėtina, suvokė, kad paspaudė netikrą nuorodą, todėl naudodamasis bendrovės programėle savo mobiliajame telefone prisijungė prie savo sąskaitos.

6. Pareiškėjas patikrinęs savo sąskaitą atsijungė, tačiau bendrovės apie pastebėtą įtartiną veiklą neinformavo.

Bendrovė pažymėjo, kad Lietuvos Respublikos mokėjimų įstatymo 34 straipsnio 1 dalyje nustatyta mokėtojo pareiga naudotis savo mokėjimo priemone pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas. Bendrovės bendrosios mokėjimo paslaugų sutarties privatiems klientams (toliau – Sutartis) 13.4 papunktyje nustatyta, kad „klientas įsipareigoja 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.“ Bendrovė teigė, kad nagrinėjamo ginčo atveju prisijungimų prie pareiškėjo paskyros istorija bei bendrovės pareiškėjo mobiliuoju telefonu siųstos SMS žinutės gavimo išrašas įrodo, kad pats pareiškėjas netinkamai apsaugojo savo prisijungimo prie paskyros duomenis ir juos atskleidė tretiesiems asmenims, dėl to ir buvo atlikta mokėjimo operacija.

Bendrovė remiasi Mokėjimų įstatymo 39 straipsnio 3 dalimi, kurioje įtvirtinta, 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 šio straipsnio 1 dalyje nustatytas didžiausios nuostolių sumos ribojimas netaikomas.

Pasisakydama dėl pareiškėjo reikalavimo grąžinti 10 Eur komisinį mokestį už mokėjimo operacijos atšaukimą, bendrovė nurodė, kad 2021 m. rugsėjo 9 d. grąžino pareiškėjui į jo sąskaitą 10 Eur komisinį mokestį už mokėjimo operacijos atšaukimą.

Atsižvelgdama į pirmiau išdėstytą informaciją, bendrovė prašo 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. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Pareiškėjo ir bendrovės ginčas kilo dėl bendrovės atsisakymo grąžinti pareiškėjui pareiškėjo vardu bendrovėje atidarytoje sąskaitoje atliktos 470 Eur mokėjimo operacijos lėšas

(toliau – ginčijama mokėjimo operacija). Pareiškėjas teigia neautorizavęs ginčijamos mokėjimo operacijos, ji atlikta be jo žinios ir sutikimo, todėl prašė bendrovės grąžinti ginčijamos mokėjimo operacijos lėšas. Bendrovė sutinka, kad ginčijama mokėjimo operacija galėjo būti inicijuota ne paties pareiškėjo, neteisėtai veikiančių trečiųjų asmenų, kurie neteisėtu būdu dėl pareiškėjo didelio aplaidumo – neišsaugotų personalizuotų saugos duomenų, 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 ginčijamą mokėjimo operaciją. Bendrovė teigia, kad jos turimi duomenys rodo, kad prisijungimas prie pareiškėjo paskyros ir sąskaitos iš kito įrenginio ir IP adreso Prancūzijoje buvo autorizuotas remiantis saugesnio autentiškumo patvirtinimo procedūra – buvo suvesti ne tik prisijungimo prie pareiškėjo paskyros duomenys (el. pašto adresas, telefono numeris ir slaptažodis), bet ir vienkartinis saugos kodas, kuris SMS žinute buvo atsiųstas į pareiškėjo bendrovei nurodytą telefono numerį. Bendrovė teigia, kad pareiškėjas neįvykdė tiek Sutarties 13.4 papunktyje nustatytos mokėtojo pareigos saugoti savo slaptažodžius ar kitokius mokėjimo priemonių personalizuotus saugumo duomenis ir jų neatskleisti tretiesiems asmenims, tiek ir Mokėjimų įstatyme 34 straipsnyje nustatytos mokėtojo pareigos saugoti savo personalizuotus saugos duomenis, taigi, dėl didelio neatsargumo neišsaugojo savo prisijungimo prie paskyros duomenų ir tretiesiems asmenis atskleidė vienkartinį saugos kodą, kurį buvo gavęs į savo mobiliojo telefono numerį.

Siekiant išspręsti tarp pareiškėjo ir bendrovės kilusį ginčą, Lietuvos banko vertinimu, būtina nustatyti šias pagrindines aplinkybes: 1) ar ginčijama mokėjimo operacija laikytina autorizuota, t. y. ar šiai mokėjimo operacijai atlikti buvo gautas pareiškėjo sutikimas; 2) ar bendrovė turėjo (turi) pareigą grąžinti pareiškėjui ginčijamos mokėjimo operacijos sumą.

Mokėjimo paslaugų teikėjų veiklą ir atsakomybę, mokėjimo paslaugas, jų teikimo sąlygas ir informavimo apie šias sąlygas reikalavimus, mokėjimo operacijų autorizavimą ir vykdymą, mokėjimo paslaugų vartotojų ir mokėjimo paslaugų teikėjų teises ir pareigas, susijusias su mokėjimo paslaugomis, kai mokėjimo paslaugų teikimas yra verslas, reglamentuoja Mokėjimų įstatymas.

Dėl ginčijamos mokėjimo operacijos 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 įstatymo 37 straipsnio 1 dalyje nustatyta, kad jeigu mokėtojas neigia autorizavęs įvykdytą mokėjimo operaciją ar teigia, kad mokėjimo operacija buvo įvykdyta netinkamai, jo mokėjimo paslaugų teikėjas turi įrodyti, kad mokėjimo operacijos autentiškumas buvo patvirtintas, ji buvo tinkamai užregistruota, įrašyta į sąskaitas ir jos nepaveikė techniniai trikdžiai arba kiti mokėjimo paslaugų teikėjo teikiamos paslaugos trūkumai; kai mokėtojas neigia autorizavęs įvykdytą mokėjimo operaciją, mokėtojo mokėjimo paslaugų teikėjo arba atitinkamais atvejais mokėjimo inicijavimo paslaugos teikėjo užregistruotas mokėjimo priemonės naudojimas nebūtinai yra pakankamas įrodymas, kad mokėtojas autorizavo mokėjimo operaciją ar veikė nesąžiningai arba tyčia ar dėl didelio neatsargumo neįvykdė vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų.

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

Pagal pareiškėjo ir bendrovės sudarytos Sutarties 8.1 papunktį, „mokėjimo operacija laikoma autorizuota tik tada, kai mokėtojas duoda sutikimą. Klientas (mokėtojas) sutikimą gali pateikti Paysera nustatyta arba Paysera ir tokio kliento sutarta forma ir būdu. Sutikimas taip pat gali būti patvirtinamas elektroniniu parašu, klientui suteiktu slaptažodžiu, kodais ir (arba) kitomis tapatybės patvirtinimo priemonėmis.“

Bendrovės teigimu, pareiškėjas ir bendrovė buvo sutarę, kad pareiškėjo sutikimas įvykdyti konkrečią mokėjimo operaciją bus duodamas naudojant tapatybės patvirtinimo priemonę. Ginčo byloje turimais duomenimis, pareiškėjas savo telefone turėjo įsidiegęs

bendrovės programėlę.

Bendrovės teigimu, iš bendrovės turimų vidinių sistemų išrašų buvo nustatyta, kad prie pareiškėjo paskyros, o kartu ir sąskaitos buvo jungtasi iš IP adreso, registruoto Prancūzijoje, ir iš kito įrenginio – mobiliojo telefono. Prisijungimas iš kito įrenginio prie pareiškėjo sąskaitos bendrovėje buvo patvirtintas suvedus pareiškėjo paskyros duomenis (el. pašto adresą, telefono numerį ir slaptažodį) ir papildomai prisijungimą iš kito įrenginio prie pareiškėjo paskyros ir sąskaitos patvirtinant vienkartiniu saugos kodu, kuris SMS žinute buvo išsiųstas į pareiškėjo bendrovei nurodytą mobiliojo telefono numerį. Bendrovės teigimu, minėti duomenys rodo, kad ginčijama mokėjimo operacija buvo autorizuota, nes ji buvo patvirtinta pareiškėjo ir bendrovės sutarta tvarka. Bendrovė paaiškino, kad, norint pasinaudojant bendrovės programėle įvykdyti mokėjimo operaciją, pakanka tik bendrovės ir kliento sutartu būdu prisijungiant prie bendrovės paskyros patvirtinti paskyros savininko tapatybę, o konkreti mokėjimo operacija yra patvirtinama bendrovės programėlėje paspaudus mygtuką „Patvirtinti".

Vis dėlto, nors bendrovė teigia, kad ginčijama mokėjimo operacija buvo patvirtinta pareiškėjo ir bendrovės Sutartyje sutarta tvarka, bendrovė pateiktame atsiliepime remiasi Mokėjimų įstatymo nuostatomis, reglamentuojančiomis neautorizuotas mokėjimo operacijas. Bendrovė pateiktame atsiliepime iš esmės pripažįsta, kad iš bendrovės surinktų duomenų matyti, kad ginčijama mokėjimo operacija galėjo būti inicijuota be pareiškėjo žinios ir sutikimo. Bendrovė pateiktame atsiliepime paaiškino, kad panašiu metu, kai buvo įvykdyta pareiškėjo ginčijama mokėjimo operacija, buvo surengta kibernetinė sukčių ataka ir iš bendrovės klientų sąskaitų buvo įvykdytos mokėjimo operacijos, kurioms bendrovės klientai teigė nedavę sutikimo. Bendrovės turimais duomenis, pareiškėjo ginčijamos mokėjimo operacijos įvykdymo aplinkybės yra iš esmės panašios ir į kitų dėl neteisėtų trečiųjų asmenų veiksmų nukentėjusių bendrovės klientų nurodytas aplinkybes.

Teiginiams, kad ginčijama mokėjimo operacija galėjo būti inicijuota ne paties pareiškėjo ir be jo žinios bei sutikimo, pagrįsti bendrovė pateikė savo vidaus sistemose užfiksuotus duomenis apie ginčijamos mokėjimo operacijos atlikimo aplinkybes.

Bendrovė Lietuvos bankui pateikė informacinės sistemos žurnalo įrašus apie užfiksuotus IP adresus, iš kurių iki ginčijamos mokėjimo operacijos atlikimo ir po jos buvo jungtasi prie pareiškėjo paskyros. Ginčijama mokėjimo operacija buvo inicijuota 2021 m. rugpjūčio 4 d. 9:04:47 val. iš IP adreso Nr. *duomenys neskelbiami*, registruoto Prancūzijoje. Iš bendrovės pateiktų išrašų matyti, kad 2021 m. rugpjūčio 3 d. 21:22:45 val. prie pareiškėjo paskyros buvo jungtasi iš IP adreso Nr. *duomenys neskelbiami*, registruoto Lietuvoje, o jau 2021 m. rugpjūčio 4 d. 8:14:47 val. prie pareiškėjo paskyros buvo jungtasi iš to paties IP adreso (*duomenys neskelbiami*), registruoto Prancūzijoje, iš kurio ir buvo įvykdyta ginčijama mokėjimo operacija. Analizuojant bendrovės Lietuvos bankui pateiktus informacinės sistemos žurnalo įrašus apie užfiksuotus IP adresus, iš kurių buvo jungtasi prie pareiškėjo paskyros, matyti, kad laikotarpiu tarp 2021 m. rugpjūčio 4 d. 8:14:47 val. ir 2021 m. rugpjūčio 4 d. 9:49:27 val., kai bendrovės sistemos užfiksavo prisijungimo prie paskyros slaptažodžio keitimą, prie pareiškėjo paskyros bendrovėje buvo jungtasi iš skirtingų IP adresų, registruotų dviejose valstybėse – Lietuvoje ir Prancūzijoje, ir iš skirtingų įrenginių. 2021 m. rugpjūčio 4 d. 8:15:11 val. prie pareiškėjo paskyros buvo jungtasi iš Lietuvoje registruoto IP adreso Nr. *duomenys neskelbiami*; 2021 m. rugpjūčio 4 d. 8:27:48 val. prie pareiškėjo paskyros buvo jungtasi iš to paties IP adreso (*duomenys neskelbiami*), registruoto Prancūzijoje, iš kurio ir buvo įvykdyta ginčijama mokėjimo operacija. Bendrovės užfiksuotais duomenimis, tą pačią 2021 m. rugpjūčio 4 d. buvo užfiksuoti dar keli prisijungimai prie pareiškėjo paskyros iš to paties IP adreso, registruoto Prancūzijoje, iki 2021 m. rugpjūčio 4 d. 9:04:47 val. inicijuotos ginčijamos mokėjimo operacijos. Po ginčijamos mokėjimo operacijos įvykdymo momento 2021 m. rugpjūčio 4 d. 9:24:18 val. prie pareiškėjo paskyros buvo prisijungta iš IP adreso Nr. *duomenys neskelbiami*, registruoto Lietuvoje. Vėliau dar buvo užfiksuoti keli prisijungimai iš to paties IP adreso, registruoto Prancūzijoje. Pareiškėjas teigė, kad prisijungė prie savo sąskaitos ir 2021 m. rugpjūčio 4 d. 8:16:21 val. autorizavo 480 Eur mokėjimą gavėjui *OÜ Company in Estonia*. Taip pat pareiškėjas pateikė IP adresų, iš kurių jis buvo jungęsis prie savo paskyros, sąrašą. Iš pareiškėjo pateiktos informacijos apie IP adresus galima teigti, kad iš IP adreso Nr. *duomenys neskelbiami* bei Nr. *duomenys neskelbiami* jungėsi pats pareiškėjas.

Iš pirmiau minėtų duomenų yra akivaizdu, kad tuo pačiu metu prie pareiškėjo paskyros buvo jungiamasi iš skirtingose valstybėse registruotų skirtingų IP adresų ir skirtingų įrenginių. Todėl iš šios informacijos galima daryti pagrįstą išvadą, kad galimybę prisijungti prie pareiškėjo paskyros ir sąskaitos bendrovėje turėjo ne tik pats pareiškėjas, bet ir tretieji asmenys, kurie

prie pareiškėjo paskyros jungėsi iš kito įrenginio ir iš kito IP adreso, registruoto Prancūzijoje.

Bendrovės teigimu, tikėtina, kad pareiškėjo prisijungimo prie paskyros duomenys galėjo būti nusavinti pareiškėjui paspaudus reklaminę nuorodą *Google* paieškos sistemoje ir į suklastotą bendrovės puslapį pavadinimu *www.paeysera.com* suvedus savo prisijungimo prie paskyros duomenis (el. pašto adresą, telefono numerį ir prisijungimo slaptažodį) bei SMS žinute gautą vienkartinį saugos kodą. Tretieji asmenys, nusavinę suklastotoje bendrovės svetainėje pareiškėjo suvestus prisijungimo prie paskyros duomenis, iš kito įrenginio ir IP adreso prisijungė prie pareiškėjo paskyros. Prisijungimas prie pareiškėjo paskyros iš naujo įrenginio buvo patvirtintas SMS žinute gautu vienkartiniu saugos kodu, kurį pareiškėjas, tikėtina, atskleidė tretiesiems asmenims. Kaip buvo minėta, bendrovės nuomone, SMS žinute gautas vienkartinis saugos kodas galėjo tapti žinomas tretiesiems asmenims, kai pareiškėjas jį suvedė į suklastotą bendrovės svetainę. Bendrovė paaiškino, kad prie savo paskyrų bendrovės klientai gali jungtis naudodamiesi kompiuteriu (per *web* naršyklę), telefonu (per *web* naršyklę / APP), planšetiniu kompiuteriu (per *web* naršyklę / APP). Bendrovė taip pat paaiškino, kad savo klientams automatiškai nesiunčia pranešimo, kad prie kliento paskyros buvo prisijungta iš kito įrenginio.

Siekdama nustatyti, kokiu būdu galėjo būti pasisavinti pareiškėjo prisijungimo prie paskyros duomenys ir vienkartinis SMS žinute bendrovės pareiškėjui atsiųstas saugos kodas, bendrovė paprašė pareiškėjo pateikti išrašą iš jo naršyklės apie naršymo internete istoriją bei nurodyti, ar pareiškėjas tretiesiems asmenims nebuvo atskleidęs savo prisijungimo prie paskyros duomenų bei SMS žinute gauto vienkartinio saugos kodo. Pareiškėjas bendrovei savo naršyklės naršymo istorijos duomenų nepateikė, taip pat nurodė, kad prisijungimo prie savo paskyros duomenų niekam nebuvo atskleidęs. Pareiškėjas bendrovei paaiškino, kad prie savo paskyros jungėsi tik per savo mobiliąją programėlę telefone, bet ne per *Google* paieškos sistemą.

Kol vyko ginčo nagrinėjimo procesas, Lietuvos bankas taip pat kreipėsi į pareiškėją ir paprašė pateikti papildomos informacijos: ar laikotarpiu, kai buvo atlikta ginčijama mokėjimo operacija, pareiškėjas spaudė nuorodą, kuri galėjo atrodyti kaip prisijungimo prie bendrovės interneto puslapio nuoroda; ar paspaudęs nuorodą pareiškėjas joje suvedė arba kam nors padiktavo prisijungimo prie savo paskyros duomenis; ar savo telefono numeriu SMS žinute gautą unikalų vienkartinį saugos kodą pareiškėjas suvedė atidarytoje nuorodoje pateiktame interneto puslapyje arba kam nors jį padiktavo. Atsakydamas į Lietuvos banko jam užduotus papildomus klausimus pareiškėjas tik nurodė, kad „jungtasi buvo tik per mobiliąją aplikaciją. Jokių prisijungimo nuorodų gavęs nesu.“ Pareiškėjas Lietuvos bankui telefonu dar papildomai paaiškino, kad nebuvo gavęs ir niekam nebuvo atskleidęs SMS žinute jo telefono numeriu siųsto vienkartinio saugos kodo, kuriuo buvo patvirtintas prisijungimas prie pareiškėjo paskyros iš kito įrenginio. Taip pat pareiškėjas pakartojo, kad prie bendrovės paskyros visą laiką jungėsi tik per mobiliąją aplikaciją savo telefone.

Bendrovė Lietuvos bankui pateikė duomenis, kurie patvirtina, kad 2021 m. rugpjūčio 4 d. 08:14:11 val. į pareiškėjo bendrovei nurodytą telefono numerį *duomenys neskelbiami* buvo išsiųsta SMS žinutė su vienkartiniu saugos kodu 270510. Iš karto po to, 2021 m. rugpjūčio 4 d. 08:14:14 val., prie pareiškėjo paskyros buvo prisijungta iš IP adreso Nr. *duomenys neskelbiami*, registruoto Prancūzijoje, o 2021 m. rugpjūčio 4 d. 08:15:11 val. prie pareiškėjo paskyros buvo prisijungta iš IP adreso Nr. *duomenys neskelbiami*, registruoto Lietuvoje.

Bendrovės pateikti ir pirmiau aptarti duomenys patvirtina faktą, kad galimybę prisijungti prie pareiškėjo paskyros ir sąskaitos turėjo ne tik pats pareiškėjas, bet ir tretieji asmenys, kurie, bendrovės turimais duomenimis, prisijungimo prie pareiškėjo paskyros duomenis galėjo iš pareiškėjo išvilioti neteisėtu būdu. Vis dėlto ginčo byloje trūksta nuodugnių pareiškėjo paaiškinimų, kaip tretieji asmenys galėjo sužinoti prisijungimo prie jo paskyros duomenis bei SMS žinute gautą vienkartinį saugos kodą. Pareiškėjas tiek bendrovei, tiek Lietuvos bankui tik nurodė, kad prie savo paskyros jungėsi tik per mobiliąją aplikaciją savo telefone, SMS žinutės su vienkartiniu kodu nebuvo gavęs ir niekam nebuvo atskleidęs savo prisijungimo prie paskyros duomenų. Nors pareiškėjas neigia, kad spaudė reklaminę nuorodą *Google* sistemoje ir iš ten pateko į netikrą bendrovės puslapį *www.paeysera.com*, kuriame suvedė savo prisijungimo prie paskyros duomenis (el. pašto adresą, tel. numerį ir prisijungimo slaptažodį) bei SMS žinute gautą vienkartinį kodą, tačiau, nors ir buvo prašoma, nepateikė duomenų iš savo naršyklės apie savo naršymo istoriją. Pareiškėjui nepateikus išsamių paaiškinimų bei prašomų duomenų, nėra galimybės tiksliai nustatyti, kokiu būdu tretiesiems asmenims galėjo tapti žinomi

pareiškėjo prisijungimo prie paskyros duomenys ir kaip tretieji asmenys galėjo iš pareiškėjo sąskaitos vykdyti neribotą kiekį mokėjimo operacijų, įskaitant ir ginčijamą mokėjimo operaciją. Apie tai, kaip tretieji asmenys galėjo prisijungti prie pareiškėjo paskyros, galima spręsti tik iš bedrovės Lietuvos bankui pateiktos informacijos, remiantis bendrovės nustatytais duomenimis daromomis prielaidomis, kaip tretieji asmenys be pareiškėjo žinios ir sutikimo galėjo įvykdyti ginčijamą mokėjimo operaciją.

Įvertinus abiejų ginčo šalių nurodytas aplinkybes ir remiantis ginčo byloje turimais įrodymais – aplinkybe, kad ginčijamos mokėjimo operacijos atlikimo metu prie pareiškėjo paskyros vienu metu buvo jungtasi iš skirtingų IP adresų, registruotų skirtingose valstybėse – Lietuvoje ir Prancūzijoje, aplinkybe, kad ginčijama mokėjimo operacija buvo inicijuota iš IP adreso Prancūzijoje, nors pareiškėjas teigia tuo pačiu metu iš IP adreso Lietuvoje inicijavęs mokėjimo operaciją, kurios neginčija, aplinkybe, kad papildomas įrenginys – mobilusis telefonas, buvo prijungtas prie pareiškėjo sąskaitos iš IP adreso, registruoto Prancūzijoje, o papildomo įrenginio prie pareiškėjo paskyros prijungimas buvo patvirtintas saugesnio autentiškumo procedūra, taip pat įvertinus tai, kad bendrovė iš esmės pripažįsta, kad ginčijamą mokėjimo operaciją iš pareiškėjo sąskaitos galėjo inicijuoti tretieji asmenys be pareiškėjo žinios ir sutikimo neteisėtu būdu pasisavinę pareiškėjo prisijungimo prie paskyros duomenis, galima daryti išvadą, kad labiau tikėtina, kad ginčijamą mokėjimo operaciją inicijavo ne pats pareiškėjas, o tretieji asmenys, kurie pasisavino pareiškėjo prisijungimo prie paskyros duomenis. Atsižvelgiant į tai, Lietuvos banko nuomone, yra pagrindas ginčijamą mokėjimo operaciją laikyti neautorizuotą.

Dėl neautorizuotų mokėjimo operacijų pasekmių ir pareiškėjo teisės į ginčijamos mokėjimo operacijų sumos grąžinimą

Vadovaujantis 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.

Bendrovė pripažįsta, kad ginčijama mokėjimo operacija iš pareiškėjo sąskaitos galėjo būti įvykdyta be pareiškėjo žinios ir sutikimo, ir teigia, kad tretieji asmenys galėjo pasisavinti pareiškėjo prisijungimo prie paskyros duomenis ir SMS žinute į pareiškėjo mobilaus telefono numerį atsiųstą vienkartinį saugos kodą, kuriuo buvo patvirtintas prisijungimas prie pareiškėjo sąskaitos iš kito įrenginio, tik dėl to, kad pareiškėjas dėl savo didelio neatsargumo neišsaugojo savo prisijungimo prie paskyros duomenų ir tretiesiems asmenims atskleidė SMS žinute gautą vienkartinį saugos kodą.

Kad būtų galima įvertinti, ar pareiškėjas iki ginčijamos mokėjimo operacijos įvykdymo galėjo pastebėti, kad mokėjimo priemonė buvo neteisėtai pasisavinta, svarbūs ne tik bendrovės pateikti sistemų išrašų duomenys apie ginčijamos mokėjimo operacijos įvykdymą, bet ir ginčo šalių paaiškinimai apie mokėjimo priemonės praradimo ir ginčijamos mokėjimo operacijos įvykdymo aplinkybes. Šiame kontekste pažymėtina, kad, kaip ir buvo minėta, pareiškėjas, nors ir prašomas, detalesnių paaiškinimų, kaip tretiesiems asmenims galėjo tapti žinomi jo

prisijungimo prie paskyros duomenys, įskaitant ir SMS žinute gautą vienkartinį saugos kodą, nei bendrovei, nei Lietuvos bankui nepateikė. Pareiškėjas tik nurodė, kad niekam savo prisijungimo prie paskyros duomenų nebuvo atskleidęs, o prie savo paskyros jungėsi tik per savo mobiliajame telefone įdiegtą bendrovės mobiliąją programėlę.

Teigdama, kad pareiškėjas dėl didelio neatsargumo galėjo parasti savo prisijungimo prie paskyros duomenis, bendrovė remiasi tiek turimais vidinių sistemų apie ginčijamos mokėjimo operacijos įvykdymo aplinkybes duomenimis, tiek turima informacija apie sukčių įvykdytos kibernetinės atakos aplinkybes, kurios, bendrovės teigimu, yra labai panašios į ginčijamos mokėjimo operacijos įvykdymo aplinkybes. Kaip jau minėta, bendrovės turimais duomenimis, labiausiai tikėtina, kad pareiškėjas galėjo prarasti savo prisijungimo prie paskyros duomenis, kai prie paskyros jungėsi per *Google* paieškos sistemą spausdamas reklaminę nuorodą *Google* paieškos sistemoje į netikrą bendrovės puslapį *www.paeysera.com* ir joje suvedė savo prisijungimo prie paskyros duomenis ir SMS žinute gautą vienkartinį saugos kodą. Pareiškėjas neigia, kad jungėsi prie savo paskyros naudodamas kokią nors kitą nuorodą, išskyrus bendrovės programėlę savo mobiliajame telefone. Vis dėlto pareiškėjo buvo prašoma pateikti naršyklės naršymo istorijos duomenis, kad būtų galima nustatyti, ar tikrai pareiškėjas prie suklastotos bendrovės paskyros nesijungė per *Google* paieškos sistemą. Bendrovė nurodė, kad pareiškėjas prašomų duomenų nepateikė. Pareiškėjas šių duomenų nepateikė ir Lietuvos bankui, tačiau pateikė IP adresų, iš kurių jis pats jungėsi prie savo paskyros, sąrašą.

Bendrovė taip pat nustatė, kad 2021 m. rugpjūčio 4 d. 08:14:11 val. į pareiškėjo bendrovei nurodytą telefono numerį *duomenys neskelbiami* buvo išsiųsta SMS žinutė su vienkartiniu saugos kodu 270510 ir iš karto po to 2021 m. rugpjūčio 4 d. 08:14:14 val. prie pareiškėjo paskyros buvo prisijungta iš Prancūzijoje registruoto IP adreso, iš kurio 2021 m. rugpjūčio 4 d. 9:04:47 val. buvo inicijuota ginčijama mokėjimo operacija. Pažymėtina, kad Lietuvos bankas pareiškėjo elektroniniu paštu teiravosi, ar jis kam nors buvo atskleidęs arba suvedęs į per *Google* paieškos sistemoje atidarytą suklastotą bendrovės svetainę savo prisijungimo prie paskyros duomenis bei SMS žinute į savo telefono numerį gautą vienkartinį saugos kodą, tačiau pareiškėjas elektroniniu laišku į šį Lietuvos banko klausimą atsakymo nepateikė ir tik telefonu nurodė, kad prie paskyros jungėsi tik per mobiliąją aplikaciją savo telefone, bei teigė, kad minėto saugos kodo SMS žinute nebuvo gavęs.

Nors pareiškėjas nurodo, kad prie savo paskyros jungėsi tik per bendrovės mobiliąją aplikaciją savo telefone, tačiau iš bendrovės Lietuvos bankui pateiktų duomenų yra akivaizdu, kad prie pareiškėjo paskyros tuo pačiu metu buvo jungiamasi iš skirtingų įrenginių ir skirtingų IP adresų, registruotų skirtingose valstybėse. Vadinasi, galimybę prisijungti prie pareiškėjo paskyros turėjo ne tik pats pareiškėjas, bet ir tretieji asmenys. Kaip ir buvo minėta, tam, kad tretieji asmenys įgytų galimybę prisijungti prie pareiškėjo paskyros, jiems turėjo būti žinomi pareiškėjo prisijungimo prie paskyros duomenys ir SMS žinute gautas vienkartinis saugos kodas, kuriuo ir buvo patvirtintas prisijungimas prie pareiškėjo sąskaitos iš kito įrenginio. Vis dėlto pareiškėjas nepateikia išsamių paaiškinimų apie ginčijamos mokėjimo operacijos įvykdymo aplinkybes ir nepateikia prašomos informacijos, patvirtinančios, kad pareiškėjas tikrai, kaip teigia, pagal bendrovės daromą prielaidą nesijungė prie savo paskyros per *Google* paieškos sistemoje atidarytą suklastotą bendrovės nuorodą *www.paeysera.com* ir joje nesuvedė savo prisijungimo prie paskyros duomenų bei SMS žinute į savo telefono numerį gauto vienkartinio saugos kodo.

Teigdama, kad pareiškėjas dėl savo didelio neatsargumo prarado prisijungimo prie paskyros duomenis bei SMS žinute gautą vienkartinį saugos kodą, bendrovė iš esmės remiasi tik prielaida, kad pareiškėjas tapo sukčių įvykdytos kibernetinės atakos auka. Kaip bendrovė pažymėjo atsiliepime Lietuvos bankui, kibernetinė ataka buvo įvykdyta tuo pačiu metu, kaip ir ginčijama mokėjimo operacija, kibernetinės atakos įvykdymo seka, aplinkybės, kuriomis ir iš kitų bendrovės klientų sąskaitų buvo inicijuotos mokėjimo operacijos, kurioms bendrovės klientai teigė nedavę sutikimo, yra panašios. Taigi, bendrovė, remdamasi turimais duomenimis apie įvykdytą kibernetinę ataką, daro prielaidą, kad pareiškėjas savo prisijungimo prie paskyros duomenis galėjo prarasti jungdamasis prie suklastotos bendrovės svetainės per *Google* paieškos sistemoje atidarytą suklastotą bendrovės nuorodą *www.paeysera.com* ir joje suvesdamas savo prisijungimo prie paskyros duomenis bei SMS žinute į savo telefono numerį gautą vienkartinį saugos kodą arba pareiškėjas galėjo tuos duomenis padiktuoti telefonu jam paskambinusiems asmenims. Tačiau pareiškėjas šių bendrovės daromų prielaidų nepatvirtina.

Atkreiptinas dėmesys, kad prisijungimo prie paskyros slaptažodis bei vienkartinis saugos kodas yra duomenys, kurie turėtų būti žinomi tik pačiam pareiškėjui, vadinasi, jų neatskleidus

tretiesiems asmenims, ginčijama mokėjimo operacija nebūtų buvusi įvykdyta. Pats pareiškėjas patvirtino, kad šie duomenys buvo žinomi tik jam vienam. Tačiau, kaip ir buvo minėta, pareiškėjas neatskleidžia, kokiu būdu tik jam vienam žinomi jo prisijungimo prie paskyros duomenys ir vienkartinis saugos kodas galėjo tapti žinomi tretiesiems asmenims, tėra bendrovės surinktais duomenimis pagrįstos prielaidos, kad labiausiai tikėtina, kad pareiškėjas savo prisijungimo prie paskyros duomenis prarado per kibernetinę sukčių ataką.

Mokėjimų įstatymo 37 straipsnio 3 dalyje nustatyta, kad kai mokėtojas neigia autorizavęs įvykdytą mokėjimo operaciją, mokėtojo mokėjimo paslaugų teikėjo arba atitinkamais atvejais mokėjimo inicijavimo paslaugos teikėjo užregistruotas mokėjimo priemonės naudojimas nebūtinai yra pakankamas įrodymas, kad mokėtojas autorizavo mokėjimo operaciją ar veikė nesąžiningai arba tyčia ar dėl didelio neatsargumo neįvykdė vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų. Mokėtojo mokėjimo paslaugų teikėjas ir atitinkamais atvejais mokėjimo inicijavimo paslaugos teikėjas turi pateikti įrodymų, kuriais patvirtinamas mokėtojo sukčiavimas arba didelis neatsargumas.

Įvertinus Mokėjimų įstatymo nuostatas, galima teigti, kad mokėtojo mokėjimo paslaugų teikėjas gali būti visiškai atleistas nuo pareigos grąžinti mokėtojui neautorizuotos mokėjimo operacijos sumą tik tada, jeigu pateikia įrodymų dėl mokėtojo sukčiavimo (nesąžiningumo arba tyčios) arba didelio neatsargumo (Mokėjimų įstatymo 37 straipsnio 3 dalis ir 39 straipsnio 3 dalis).

Pažymėtina, kad šalių ginčo dėl to, kad pareiškėjas galėjo veikti nesąžiningai arba tyčia, įskaitant sukčiavimą, nėra. Tai reiškia, kad, siekiant įvertinti, ar šiuo atveju pareiškėjo atžvilgiu galėtų būti taikoma Mokėjimų įstatymo 39 straipsnio 3 dalis, būtina nustatyti, ar pareiškėjo elgesys, prarandant mokėjimo priemonę ir jos personalizuotus saugos duomenis, gali būti vertinamas kaip didelis pareiškėjo neatsargumas (aplaidumas), dėl kurio visi nuostoliai, susiję su ginčijamų mokėjimo operacijų įvykdymu, turėtų tekti pareiškėjui.

Šiame kontekste pažymėtina ir tai, kad aplaidumo laipsnio vertinimas yra susijęs su asmens pareigos elgtis atidžiai ir rūpestingai konkrečioje situacijoje vertinimu. Tam, kad būtų galima įvertinti, ar konkretūs pareiškėjo veiksmai parandant mokėjimo priemonę gali būti vertinami kaip labai aplaidūs arba tik aplaidūs, yra labai svarbus ginčo šalių bendradarbiavimas sprendžiant konkrečią ginčo situaciją ir kuo išsamesnės informacijos apie ginčijamos mokėjimo operacijos įvykdymo aplinkybes pateikimas.

Antrosios mokėjimo paslaugų direktyvos (toliau – PSD2) preambulės 72 punkte rašoma, kad „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 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).

Ginčo bylos duomenys patvirtina, kad bendrovė ginčijamai mokėjimo operacijai inicijuoti taikė saugesnio autentiškumo nustatymo procedūrą. Labiausiai tikėtina, kad pats pareiškėjas neužtikrino savo personalizuotų saugumo duomenų konfidencialumo. Toks pareiškėjo elgesys galėjo lemti tai, kad bendrovės taikyta saugesnio autentiškumo patvirtinimo procedūra šiuo atveju nebuvo pakankama tam, kad iš pareiškėjo sąskaitos nebūtų įvykdyta ginčijama mokėjimo operacija, kuriai pareiškėjas teigia nedavęs sutikimo.

Kita vertus, aplinkybė, kad ginčijama mokėjimo operacija buvo patvirtinta, naudojant mokėjimo operacijoms autorizuoti šalių sutartiniuose santykiuose sutartas naudoti saugesnio autentiškumo nustatymo priemones, šiuo atveju esant įrodymų, kad labiausiai tikėtina, kad šalių sutarta mokėjimo operacijos saugesnio autentiškumo patvirtinimo procedūra tretieji asmenys galėjo pasinaudoti be pareiškėjo žinios ir sutikimo, nesudaro pakankamo pagrindo teigti, kad tokia mokėjimo operacija autorizuota, bet kartu ir savaime nesuponuoja išvados, kad pareiškėjo elgesys prarandant mokėjimo priemonę (labiausiai tikėtina, įgalinant trečiuosius asmenis prisijungti prie pareiškėjo paskyros iš kito įrenginio) vertintinas kaip labai neatsargus.

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.

Kaip ir buvo minėta pirmiau, ginčo byloje nėra pareiškėjo paaiškinimų apie jo elgesį, lėmusį tai, kad buvo prarasta mokėjimo priemonė, todėl tokius pareiškėjo veiksmus galima vertinti tik kartu su bendrovės pateiktais vidinių sistemų išrašais ir daromomis prielaidomis, kaip pareiškėjas galėjo prarasti mokėjimo priemonę, o tretieji asmenys pasinaudodami iš pareiškėjo nusavintais personalizuotais saugos duomenimis galėjo įvykdyti ginčijamą mokėjimo operaciją.

Kaip buvo minėta, bendrovė iš turimos informacijos daro prielaidą, kad, nors pareiškėjas tai neigia, jis *Google* paieškos sistemoje paspaudė suklastotos bendrovės paskyros nuorodą *www.paeysera.com* ir joje suvedė tiek prisijungimo prie savo paskyros duomenis, tiek SMS žinute gautą vienkartinį saugos kodą, kuriuo buvo patvirtintas trečiųjų asmenų prisijungimas prie pareiškėjo paskyros iš kito įrenginio. Bendrovė taip pat teigia, kad yra tikimybė, kad personalizuotus saugos duomenis pareiškėjas galėjo atskleisti telefonu jam paskambinusiems tretiesiems asmenims. Bendrovės nuomone, toks pareiškėjo elgesys gali būti vertinamas kaip labai neatsargus, nes tikrasis bendrovės interneto puslapio adresas yra ne *www.paeysera.com*, o *www.bank.paysera.com*, todėl vien tik neteisingas bendrovės interneto puslapio adresas pareiškėjui turėjo sukelti įtarimų, jeigu pareiškėjas būtų buvęs pakankamai atidus. Bendrovė taip pat teigė, kad didelį pareiškėjo neatsargumą suklastotoje bendrovės svetainėje suvedant savo prisijungimo prie paskyros duomenis rodo ir tas faktas, kad prisijungusiųjų prie tikros bendrovės svetainės *www.bank.paysera.com* neprašoma įvesti SMS žinute siunčiamo vienkartinio saugos kodo.

Vertinant, ar pareiškėjo elgesį, atskleidžiant tretiesiems asmenis savo prisijungimo prie paskyros duomenis bei SMS žinute gautą vienkartinį saugos kodą, galima vertinti kaip labai neatsargų, svarbus Sutarties 5.1 papunktis: „Klientas Paysera Sąskaitą gali valdyti internetu, prisijungęs prie savo Paskyros savo prisijungimo vardu ir Slaptažodžiu bei atlikęs papildomo prisijungimo (saugesnio autentiškumo patvirtinimo) procedūrą," Taigi, pareiškėjui turėjo būti žinoma, kad SMS žinute gautas vienkartinis saugos kodas yra skirtas tam, kad būtų patvirtintas prisijungimas prie jo paskyros bei sąskaitos. Kaip ir buvo minėta, ginčo byloje nėra pateikta pareiškėjo paaiškinimų, kokiu būdu SMS žinute į jo telefono numerį atsiųstas vienkartinis saugos kodas, kuriuo ir buvo patvirtintas trečiųjų asmenų prisijungimas prie pareiškėjo paskyros, tapo žinomas tretiesiems asmenims, labiausiai tikėtina, kad pareiškėjas savo prisijungimo prie paskyros duomenis prarado juos suvedęs į sukčių suklastotą svetainę *www.paeysera.com*. Objektyviai vertinant bendrovės pateiktą informaciją, kad akivaizdžiai skyrėsi bendrovės tikrosios interneto svetainės adresas nuo sukčių suklastotos, bei vertinant Sutarties 5.1 papunkčio sąlygą, kad, suvedus prisijungimo prie paskyros duomenis ir slaptažodį bei atlikus papildomo prisijungimo saugesnio autentiškumo patvirtinimo procedūrą, yra suteikiama teisė valdyti sąskaitą, galima teigti, kad pareiškėjas, tikėtina, paspausdamas nuorodą *www.paeysera.com* ir atidarytoje sukčių suklastotoje bendrovės svetainėje suvesdamas prisijungimo prie paskyros duomenis ir SMS žinute gautą vienkartinį saugos kodą, turėjo suprasti, kad tvirtina prisijungimą prie savo paskyros kitu būdu nei per mobiliajame telefone įdiegtą bendrovės aplikaciją ir taip suteikia teisę valdyti paskyrą, kartu ir vykdyti mokėjimo operacijas. Tačiau pareiškėjas, nors turėjo suprasti, kad SMS žinute gautas vienkartinis saugos kodas yra skirtas patvirtinti prisijungimą prie paskyros ir kartu pavirtinti teisės ją valdyti suteikimą kitu būdu nei per mobiliajame telefone įdiegtą bendrovės aplikaciją, tikėtina, atskleidė jį tretiesiems asmenims, todėl neišsaugojo savo personalizuotų saugos duomenų.

Kaip minėta, tiek Mokėjimų įstatymo 34 straipsnyje, tiek Sutarties 8.1 papunktyje nustatyta pareiga mokėtojui saugoti savo personalizuotus saugos duomenis ir niekam jų neatskleisti. Ginčo nagrinėjimo metu konstatuota, kad pareiškėjas neišsaugojo savo mokėjimo priemonės personalizuotų saugumo duomenų konfidencialumo ir juos atskleidė tretiesiems asmenims. Svarstant, ar pareiškėjo elgesį tretiesiems asmenims atskleidžiant personalizuotus saugumo duomenis būtų galima vertinti kaip labai neatsargų (aplaidų), ar tik neatsargų, svarbu

tai, kad nors pareiškėjas nepateikė jokių paaiškinimų apie ginčijamos mokėjimo operacijos įvykdymo aplinkybes, tačiau iš bendrovės pateiktų duomenų galima teigti, kad pareiškėjo elgesys prarandant personalizuotus saugos duomenis gali būti vertinamas kaip labai neatsargus (aplaidus) elgesys.

Ginčo byloje turimi duomenys leidžia teigti, kad labiausiai tikėtina, kad pareiškėjas prie bendrovės paskyros jungėsi *Google* paieškos sistemoje paspausdamas suklastotos bendrovės paskyros nuorodą *www.paeysera.com* ir joje suvesdamas tiek prisijungimo prie savo paskyros duomenis, tiek SMS žinute gautą vienkartinį saugos kodą, kuriuo buvo patvirtintas trečiųjų asmenų prisijungimas prie pareiškėjo paskyros iš kito įrenginio. Sukčių suklastotas bendrovės interneto svetainės adresas skyrėsi nuo tikrojo bendrovės interneto svetainės adreso *www.bank.paysera.com*, tačiau tikėtina, kad pareiškėjas to nepastebėjo. Vis dėlto pareiškėjas nepatvirtino, kad prie savo paskyros galėjo jungtis paspausdamas suklastotos bendrovės interneto svetainės nuorodą *www.paeysera.com*. Pareiškėjas tik teigia, kad prie savo paskyros jungėsi per bendrovės programėlę, įdiegtą mobiliajame telefone. Vis dėlto bendrovės sistemų išrašai įrodo, kad prie pareiškėjo paskyros tuo pačiu metu buvo jungiamasi iš dvejų įrenginių ir dvejų IP adresų, registruotų skirtingose valstybėse.

Kaip ir buvo nustatyta pirmiau, nors pareiškėjas neigia kam nors atskleidęs savo personalizuotus saugos duomenis, turimi duomenys patvirtina, kad prisijungimas prie pareiškėjo sąskaitos iš kito įrenginio ir kito IP adreso buvo patvirtintas saugesnio autentifikavimo procedūra, t. y. buvo suvesti ne tik prisijungimo prie paskyros duomenys, bet ir pats prisijungimas patvirtintas SMS žinute gautu vienkartiniu saugos kodu. Vadinasi, tam, kad tretieji asmenys įgytų galimybę prisijungti prie pareiškėjo paskyros iš kito įrenginio, pareiškėjas turėjo neišsaugoti savo prisijungimo prie paskyros duomenų ir juos atskleisti tretiesiems asmenims. Pareiškėjas nepateikia paaiškinimų, kokiu būdu tretiesiems asmenims galėjo tapti žinomi, kaip teigia pareiškėjas, tik jam vienam žinomi jo personalizuoti saugumo duomenys. Kita vertus, nustatyta, kad prisijungimas prie pareiškėjo paskyros buvo patvirtintas SMS žinute pareiškėjo telefonu gautu vienkartiniu saugos kodu. Iš ginčo byloje turimų aplinkybių visumos darytina išvada, kad labiausiai tikėtina, kad pareiškėjas šį SMS žinute tik vienam pareiškėjui žinomą vienkartinį saugos kodą atskleidė tretiesiems asmenims, nors, būdamas atidus ir rūpestingas, pareiškėjas turėjo ir galėjo suprasti, kad SMS žinute gautas vienkartinis saugos kodas yra skirtas patvirtinti prisijungimą prie jo paskyros iš kito įrenginio. Iš esmės, suteikus galimybę prisijungti prie paskyros, suteikiama ir galimybė iš sąskaitos inicijuoti mokėjimo operacijas. Pareiškėjas turėjo suprasti, kokias pasekmes gali sukelti SMS žinute gauto vienkartinio saugos kodo atskleidimas tretiesiems asmenims. Vis dėlto, nors turėjo suprasti SMS žinute gauto vienkartinio saugos kodo atskleidimo tretiesiems asmenims pasekmes, pareiškėjas SMS žinute gautą vienkartinį saugos kodą atskleidė tretiesiems asmenims, dėl to jie įgijo galimybę iš kito įrenginio ir kito IP adreso prisijungti prie pareiškėjo sąskaitos ir inicijuoti ginčijamą mokėjimo operaciją.

Vertinant nustatytų aplinkybių visumą, galima daryti išvadą, kad pareiškėjo elgesys, kai buvo prarasti personalizuoti saugos duomenys, gali būti vertinamas kaip labai neatsargus (aplaidus), t. y. neatitinkantis elementarių atidumo ir rūpestingumo reikalavimų, jis ir nulėmė tai, kad tretieji asmenys įgijo galimybę prisijungti prie pareiškėjo paskyros ir įvykdyti ginčijamą mokėjimo operaciją. Tokia išvada daroma ne tik įvertinus surinktų duomenų apie ginčijamos mokėjimo operacijos įvykdymo aplinkybes visumą, bet ir tai, kad pareiškėjas nepateikė jokių paaiškinimų, kurie leistų pareiškėjo elgesį vertinti tik kaip neatsargų. Kaip ir buvo minėta pirmiau, vertinimas, ar konkrečių individualių ginčijamos mokėjimo operacijos inicijavimo aplinkybių kontekste konkretus mokėtojo elgesys, dėl kurio buvo prarasta mokėjimo priemonė ir inicijuota ginčijama mokėjimo operacija, gali būti vertinamas kaip labai neatsargus ar tik neatsargus elgesys, yra susijęs su asmens, kuris prarado mokėjimo priemonę, elgesio konkrečioje situacijoje vertinimu atsižvelgiant į tai, ar buvo laikomasi pareigos elgtis atidžiai ir rūpestingai. Tam, kad būtų galima įvertinti mokėtojo elgesį, dėl kurio buvo prarasta mokėjimo priemonė, yra labai svarbu, kad pats mokėtojas bendradarbiautų ir pateiktų kuo išsamesnę informaciją apie savo veiksmus, dėl kurių galėjo būti parasta jo mokėjimo priemonė. Tačiau, nors pareiškėjas iš esmės neigia, kad tretiesiems asmenims atskleidė savo prisijungimo prie paskyros duomenis bei SMS žinute gautą vienkartinį saugos kodą, kuriuo buvo patvirtintas trečiųjų asmenų prisijungimas prie pareiškėjo paskyros iš kito įrenginio, tačiau iš esmės nepateikia jokių paaiškinimų bei įrodymų, kokiu būdu tretieji asmenys iš pareiškėjo galėjo pasisavinti jo mokėjimo priemonę. Pareiškėjo bendradarbiavimo nagrinėjamoje ginčo situacijoje trūkumas iš esmės ir lemia tai, kad neturima duomenų, iš kurių pareiškėjo elgesį

prarandant mokėjimo priemonę būtų galima vertinti tik kaip neatsargų ir todėl visi dėl ginčijamos mokėjimo operacijos patirti nuostoliai turėtų tekti bendrovei.

Įvertinus pirmiau išdėstytą informaciją, konstatuotina, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, kurioje nustatyta, kad mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai, jeigu jis juos patyrė dėl didelio neatsargumo neįvykdęs vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų, todėl, Lietuvos banko vertinimu, bendrovė neprivalo pareiškėjui grąžinti neautorizuotų mokėjimo operacijų lėšų, todėl pareiškėjo reikalavimas atmestinas.

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 pareiškėjo X.X. reikalavimą.

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

Direktorius Arūnas Raišutis