



**LIETUVOS BANKO
TEISĖS IR LICENCIJAVIMO DEPARTAMENTO
DIREKTORIUS**

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

2022-09-23 Nr. 429-479
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:

Pareiškėjas ir bendrovė yra sudarę mokėjimo paslaugų teikimo sutartį (toliau – Sutartis), kurios pagrindu pareiškėjui atidaryta mokėjimo sąskaita Nr. (*duomenys neskelbiami*) (toliau – sąskaita), sukurta asmeninė paskyra bendrovėje (toliau – paskyra) ir suteikta teisė naudotis kitomis mokėjimo paslaugomis.

2022 m. balandžio 9 d. 15 val. 27 min. bendrovė pareiškėjo elektroninio pašto adresu (*duomenys neskelbiami*) (toliau – el. paštas) išsiuntė pranešimą, kad prie pareiškėjo paskyros buvo prisijungta iš naujo IP adreso Nr. (*duomenys neskelbiami*) (toliau – IP Nr. 1), ir paprašė pareiškėjo nedelsiant pakeisti prisijungimo prie paskyros ir savo elektroninio pašto slaptažodžius, jeigu prie paskyros iš IP Nr. 1 jungėsi ne pats pareiškėjas (toliau – įspėjimas apie prisijungimą prie paskyros iš kito IP). Prie paskyros prisijungta iš įrenginio, kuriame įdiegta iOS programinė įranga (toliau – *Iphone* įrenginys).

2022 m. balandžio 13 d. 14 val. 32 min. 59 sek., naudojant įrenginį, kuriame įdiegta *Android* programinė įranga, (toliau – *Android* įrenginys) pakeistas prisijungimo prie pareiškėjo paskyros slaptažodis. Slaptažodžio keitimo metu prisijungta iš IP adreso Nr. (*duomenys neskelbiami*) (toliau – IP Nr. 2). Apie slaptažodžio pakeitimą bendrovė iš karto informavo pareiškėją SMS žinute, išsiųsta pareiškėjo mobiliojo telefono numeriu (*duomenys neskelbiami*) (toliau – telefono numeris).

2022 m. balandžio 13 d. 14 val. 33 min. bendrovė išsiuntė pareiškėjo telefono numeriu SMS žinutę, kad pakeistas prisijungimo prie pareiškėjo paskyros slaptažodis.

2022 m. balandžio 13 d. 14 val. 33 min. 2 sek. prie pareiškėjo paskyros prisijungta, panaudojant *Android* įrenginį, iš IP Nr. 2.

2022 m. balandžio 13 d. 14 val. 33 min. 15 sek. bendrovė išsiuntė pareiškėjo telefono numeriu SMS žinutę su vienkartinio saugos kodu, skirtu prisijungti prie pareiškėjo sąskaitos.

2022 m. balandžio 13 d. 14 val. 33 min. 45 sek. bendrovės pareiškėjo telefono numeriu išsiųstoje SMS žinutėje nurodytu vienkartinio saugos kodu iš IP Nr. 2, naudojant *Android* įrenginį, buvo patvirtintas prisijungimas prie pareiškėjo sąskaitos.

2022 m. balandžio 13 d. 14 val. 37 min. iš pareiškėjo sąskaitos buvo atliktas momentinis 4 200 EUR mokėjimas (toliau – ginčijamas mokėjimas) į gavėjos Y. Y. (toliau – gavėja) mokėjimo sąskaitą, esančią *N26 Bank GmbH* (toliau – gavėjos bankas arba N26 bankas). Ginčijamas mokėjimas inicijuotas ir patvirtintas iš IP Nr. 2, naudojant *Android* įrenginį.

2022 m. balandžio 13 d. 14 val. 37 min. 30 sek., naudojant *Android* įrenginį, nuo pareiškėjo paskyros buvo atsijungta. Atsijungta iš IP Nr. 2.

2022 m. balandžio 13 d. 15 val. 27 min. 9 sek. bendrovė išsiuntė pareiškėjo telefono numeriu SMS žinutę su vienkartinio saugos kodu, skirtu keičiamam jungimosi prie paskyros slaptažodžiui patvirtinti.

2022 m. balandžio 13 d. 15 val. 27 min. 19 sek., naudojant *Iphone* įrenginį, buvo pakartotinai pakeistas prisijungimo prie pareiškėjo paskyros slaptažodis. Slaptažodžio keitimo metu prisijungta iš IP adreso Nr. (*duomenys neskelbiami*) (toliau – IP Nr. 3).

2022 m. balandžio 13 d. 15 val. 27 min. 20 sek. bendrovė išsiuntė pareiškėjo telefono numeriu SMS žinutę, kad pakeistas prisijungimo prie pareiškėjo paskyros slaptažodis.

2022 m. balandžio 13 d. 15 val. 27 min. 30 sek. bendrovė išsiuntė pareiškėjo telefono numeriu SMS žinutę su vienkartinio saugos kodu, skirtu prisijungimui prie pareiškėjo sąskaitos patvirtinti.

2022 m. balandžio 13 d. 15 val. 27 min. 59 sek. bendrovės pareiškėjo telefono numeriu išsiųstoje SMS žinutėje nurodytu vienkartinio saugos kodu iš IP Nr. 3, naudojant *Iphone* įrenginį, buvo patvirtintas prisijungimas prie pareiškėjo sąskaitos ir prie jos prisijungta.

2022 m. balandžio 13 d. 15 val. 30 min. pareiškėjas telefonu kreipėsi į bendrovę, informavo, kad ginčijamą mokėjimą atliko ne jis, ir prašė atšaukti šį mokėjimą.

2022 m. balandžio 14 d. 8 val. 6 min. bendrovė kreipėsi į gavėjos banką dėl ginčijamo mokėjimo atšaukimo ir lėšų gražinimo pareiškėjui, tačiau tos pačios dienos 12 val. 33 min. gavo gavėjos banko atsakymą, kad ginčijamo mokėjimo atšaukimas yra negalimas, nes gavėjos mokėjimo sąskaitoje gražintinų lėšų nebėra.

Bendrovės paprašytas pateikti papildomus paaiškinimus dėl ginčijamo mokėjimo atlikimo aplinkybių, pareiškėjas nurodė prie paskyros įprastai jungęsis per bendrovės mobiliąją programėlę iš savo *Iphone* įrenginio, iki ginčijamo mokėjimo negavęs ir nespaukęs jokių nuorodų į suklastotas interneto svetaines, neatskleidęs tretiesiems asmenims prisijungimo prie paskyros duomenų ir (ar) kitu būdu nesuteikęs tretiesiems asmenims prieigos prie savo paskyros.

2022 m. gegužės 2 d. bendrovė informavo pareiškėją, kad ginčijamo mokėjimo lėšos pareiškėjui nebus gražintos.

Nesutikdamas su bendrovės atsakymu, pareiškėjas kreipėsi į Lietuvos banką dėl vartojimo ginčo nagrinėjimo. Kreipimesi nurodė, kad 2022 m. balandžio 13 d. 12 val. 33 min. gavo iš bendrovės SMS žinutę, kad prisijungimo prie jo paskyros slaptažodis yra pakeistas, naudojant *Android* įrenginį, tai jam sukėlė įtarimą, nes jis naudoja *Iphone* įrenginį, o ne *Android* įrenginį. Pareiškėjas mėgino prisijungti prie paskyros, naudodamasis veido atpažinimo autentifikacija, tačiau dėl pakeisto slaptažodžio to padaryti negalėjo, todėl dar kartą pats pakeitė prisijungimo prie savo paskyros bendrovėje slaptažodį, sėkmingai prisijungė prie paskyros ir tuomet pamatė, kad jo sąskaitoje buvo atlikta ginčijama mokėjimo operacija. Pareiškėjas ta pačią dieną nedelsdamas susisieikė su bendrove ir informavo, kad ginčijamo mokėjimo neautorizavo. Pareiškėjas nurodė nesutinkantis su bendrovės teigimu, kad jis paspaudė sukčių atsiųstoje SMS žinutėje pateiktą nuorodą, joje atskleidė prisijungimo prie paskyros slaptažodžius ir taip suteikė sukčiams prieigą prie savo paskyros, o jie vėliau atliko ginčijamą mokėjimą. Pareiškėjas pabrėžė, kad nespaukę jokių nuorodų ir prisijungimo duomenų niekur nevedė, taip pat kitu būdu neperdavė šių duomenų tretiesiems asmenims. Pareiškėjas taip pat nurodė, kad SMS žinutę su įtartina nuoroda iš to paties telefono numerio, kuriuo bendrovė įprastai siunčia jam SMS žinutes, gavo 2022 m. balandžio 18 d., tačiau jos neatidarė ir nedelsdamas paskambino bendrovei, kurios buvo informuotas neatidaryti šios nuorodos. Pareiškėjo teigimu, pati bendrovė pripažino pareiškėjui, kad prieš ją įvyko kibernetinė ataka, kurios metu sukčiai įgijo prieigą prie pareiškėjo paskyros ir padarė neautorizuotą mokėjimą į pareiškėjui nepažįstamo gavėjo mokėjimo sąskaitą, t. y. ginčijamą mokėjimą. Pareiškėjo įsitikinimu, tai įrodo, kad bendrovė nėra įdiegusi pakankamo jos vidaus sistemų saugumo, užkertančio kelią tokioms kibernetinėms atakoms, taip sudarydama tretiesiems asmenims galimybę neteisėtai prisijungti prie klientų mokėjimo sąskaitų bendrovėje ir pasisavinti šiose mokėjimo sąskaitose esančias lėšas, todėl turi gražinti pareiškėjui ginčijamo mokėjimo lėšas.

Bendrovė Lietuvos bankui pateiktame atsiliepime nurodė sutinkanti, kad pareiškėjas neautorizavo ginčijamo mokėjimo, tačiau mananti, kad ginčijamas mokėjimas buvo atliktas dėl paties pareiškėjo didelio neatsargumo, todėl bendrovė neturi pareigos gražinti pareiškėjui ginčijamo mokėjimo sumos.

Bendrovė paaiškino, kad jos vidinio tyrimo metu surinkta informacija leidžia daryti išvadą, kad pareiškėjas, priešingai, nei jis pats teigia, 2022 m. balandžio 9 d. vis dėlto paspaudė jam trečiųjų asmenų SMS žinute atsiųstą nuorodą <https://clk.one/h5Wt> (toliau – Nuoroda), per ją pateko į trečiųjų asmenų suklastotą interneto svetainę <https://paysera.cc/en/login> (toliau – Suklastota svetainė), joje suvedė prisijungimo prie savo paskyros duomenis, tačiau juos pasisavino tretieji asmenys ir 2022 m. balandžio 13 d., panaudodami šiuos duomenis, prisijungė prie pareiškėjo sąskaitos iš *Android* įrenginio ir iš jos atliko ginčijamą mokėjimą. Tokį savo teiginį bendrovė grindžia jos vidaus sistemose 2022 m. balandžio 9 d. užfiksuoto jungimosi prie pareiškėjo paskyros, kuris buvo inicijuotas iš Suklastotos svetainės, duomenimis. Nurodytą dieną prie pareiškėjo paskyros buvo prisijungta

naudojant *Iphone* įrenginį iš IP Nr. 1, kuris skyrėsi nuo IP adreso, iš kurio pareiškėjas įprastai jungėsi prie savo paskyros, todėl bendrovė iš karto po tokio prisijungimo nurodytu el. paštu pareiškėjui nusiuntė Įspėjimą apie prisijungimą prie paskyros iš kito IP. Be to, trečiųjų asmenų prisijungimas prie pareiškėjo sąskaitos 2022 m. balandžio 13 d. buvo patvirtintas bendrovės pareiškėjo telefono numeriu tą dieną 14 val. 33 min. 15 sek. SMS žinute išsiųstu vienkartinio saugos kodu. Bendrovės įsitikinimu, SMS žinute gautą vienkartinį saugos kodą pareiškėjas turėjo suvesti Suklastotoje svetainėje, taip atskleidždamas jį tretiesiems asmenims bei suteikdamas šiems asmenims visišką prieigą prie savo sąskaitos, įskaitant galimybę atlikti ginčijamą mokėjimą. Vienkartinio saugos kodo tretiesiems asmenims atskleidimo faktą, bendrovės teigimu, patvirtina bendrovės vidaus sistemoje 2022 m. balandžio 13 d. 14 val. 33 min. 2 sek. užfiksuotas trečiųjų asmenų prisijungimas prie pareiškėjo sąskaitos iš IP Nr. 2, panaudojant *Android* įrenginį. Bendrovės įsitikinimu, pareiškėjui nepaspaudus trečiųjų asmenų jam SMS žinute atsiųstos Nuorodos ir Suklastotoje svetainėje nepasidalijus su jais prisijungimo prie pareiškėjo paskyros duomenimis, įskaitant bendrovės pareiškėjui SMS žinute siųstą vienkartinį saugos kodą, tretieji asmenys nebūtų įgiję galimybės iš pareiškėjo sąskaitos atlikti ginčijamo mokėjimo.

Bendrovės nuomone, pareiškėjas turėjo įtarti, kad SMS žinutę su Nuoroda į Suklastotą svetainę pareiškėjui siuntė ne bendrovė, nes bendrovė tokio formato žinučių su nuorodomis nesiunčia, ir net jei būdamas nepakankamai atidus pareiškėjas neatkreipė dėmesio į tai, kad Suklastotos svetainės adresas akivaizdžiai skiriasi nuo tikrojo, jam turėjo kilti įtarimų dėl bendrovės pareiškėjui SMS žinute siųsto pranešimo, prašančio patvirtinti prisijungimą prie pareiškėjo paskyros iš kito, negu pareiškėjas naudoja, įrenginio. Bendrovės įsitikinimu, pareiškėjo veiksmai, kai jis net kelis kartus pasidalijo prisijungimo prie savo paskyros ir sąskaitos duomenimis su trečiaisiais asmenimis, turėtų būti vertinami kaip didelis pareiškėjo neatsargumas, dėl kurio visi nuostoliai dėl ginčijamo mokėjimo įvykdymo turėtų tekti pačiam pareiškėjui.

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

Vadovaujantis Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių, patvirtintų Lietuvos banko valdybos 2012 m. sausio 26 d. nutarimu Nr. 03-23, 45 punktu, vartojimo ginčai Lietuvos banke nagrinėjami laikantis rungimosi, ginčų nagrinėjimo operatyvumo, koncentracijos, ekonomiškumo ir bendradarbiavimo principų. Vartotojas ir finansų rinkos dalyvis privalo įrodyti tas aplinkybes, kuriomis remiasi kaip savo reikalavimų arba atsikirtimų pagrindu, išskyrus atvejus, kai remiamasi aplinkybėmis, kurių nereikia įrodinėti. Lietuvos bankas ginčo nagrinėjimo proceso metu neatlieka Lietuvos Respublikos Lietuvos banko įstatymo 42¹ straipsnyje reglamentuotų patikrinimų, skirtų faktinėms aplinkybėms, susijusioms su Lietuvos banko prižiūrimo finansų rinkos dalyvio galimu Lietuvos banko kompetencijai priskirtų teisės aktų reikalavimų pažeidimu, nustatyti ir įvertinti. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą ir jo pagrindu priima sprendimą.

Pareiškėjo ir bendrovės ginčas kilo dėl bendrovės atsisakymo gražinti pareiškėjui ginčijamo mokėjimo, atlikto iš pareiškėjo sąskaitos, sumą (iš viso 4 200 EUR).

Pareiškėją ir banką sieja sutartiniai santykiai, kylantys iš mokėjimo paslaugų teikimo. Mokėjimo paslaugų teikėjų veiklą, mokėjimo paslaugų teikimą, mokėjimo operacijų autorizavimą ir vykdymą, mokėjimo paslaugų vartotojų ir mokėjimo paslaugų teikėjų teises ir pareigas, susijusias su mokėjimo paslaugomis, kai mokėjimo paslaugų teikimas yra verslas, reglamentuoja Lietuvos Respublikos mokėjimų įstatymas.

Įvertinus ginčo šalių pateiktą informaciją ir ją pagrindžiančius įrodymus, darytina išvada, kad tarp šalių nėra ginčo dėl to, kad pareiškėjas neautorizavo ginčijamo mokėjimo. Atsižvelgiant į tai, su ginčijamo mokėjimo autorizavimo vertinimu susijusios aplinkybės šiame sprendime toliau nebus analizuojamos, laikant, kad ginčijamas mokėjimas buvo neautorizuotas, t. y. atliktas be pareiškėjo sutikimo, kaip tai suprantama Mokėjimų įstatymo 29 straipsnio 2 dalyje.

Vadovaujantis Mokėjimų įstatymo 38 straipsnio 1 dalimi, nesant Mokėjimų įstatymo 39 straipsnio 1 ir 3 dalyje nustatytų aplinkybių, mokėtojo mokėjimo paslaugų teikėjas privalo gražinti mokėtojui visą neautorizuotos mokėjimo operacijos sumą ne vėliau kaip iki 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). 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 to paties įstatymo 34 straipsnyje nustatytų pareigų, susijusių su mokėjimo priemonėmis ir personalizuotais saugumo duomenimis (Mokėjimų įstatymo 39 straipsnio 3 dalis). Mokėjimų įstatymo 34 straipsnis nustato mokėtojui, kuriam išduota mokėjimo priemonė, pareigą naudotis šia mokėjimo priemone pagal jos išdavimą ir naudojimą reglamentuojančias sąlygas, o sužinojus apie jos praradimą, vagystę arba neteisėtą pasisavinimą ar neautorizuotą jos naudojimą, nedelsiant apie tai pranešti mokėjimo paslaugų teikėjui arba jo nurodytam subjektui (Mokėjimų įstatymo 34 straipsnio 1 dalis), taip pat, gavus mokėjimo priemonę, imtis veiksmų, kad būtų apsugoti personalizuoti saugumo duomenys (Mokėjimų įstatymo 34 straipsnio 2 dalis). Vadovaujantis Mokėjimų įstatymo 37 straipsnio 1 ir 3 dalimis, pareiga 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, tenka mokėtojo mokėjimo paslaugų teikėjui. Mokėjimų įstatymo 39 straipsnio 4 dalyje nustatyta, kad, kai mokėtojo mokėjimo paslaugų teikėjas nereikalauja saugesnio autentiškumo patvirtinimo, mokėtojui dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai tenka tik tuo atveju, jeigu jis veikė nesąžiningai.

Įvertinus pirmiau nurodytas Mokėjimų įstatymo nuostatas, galima teigti, kad mokėtojo mokėjimo paslaugų teikėjas gali būti visiškai atleistas nuo pareigos gražinti mokėtojui neautorizuotos mokėjimo operacijos sumą tik tada, kai įrodomas mokėtojo sukčiavimas (nesąžiningumas arba tyčia) arba didelis neatsargumas (Mokėjimų įstatymo 37 straipsnio 3 dalis ir 39 straipsnio 3 dalis), ir (arba) tik tada, kai mokėtojo mokėjimo paslaugų teikėjas nereikalauja saugesnio autentiškumo patvirtinimo ir nenustatomas pareiškėjo nesąžiningumas (Mokėjimų įstatymo 39 straipsnio 4 dalis).

Nagrinėjamo ginčo atveju bendrovė, prašydama atmesti pareiškėjo reikalavimą, remiasi Mokėjimų įstatymo 39 straipsnio 3 dalyje įtvirtinta aplinkybe, t. y. mokėtojo dideliu neatsargumu, kuriam esant, mokėtojo mokėjimo paslaugų teikėjas yra atleidžiamas nuo pareigos gražinti mokėtojui neautorizuotos mokėjimo operacijos sumą, o dėl neautorizuotos mokėjimo operacijos atsiradę nuostoliai tenka mokėtojui. Bendrovės teigimu, pareiškėjo didelis neatsargumas pasireiškė tuo, kad jis paspaudė trečiųjų asmenų jam SMS žinute siųstą Nuorodą, nukreipiančią į Suklastotą svetainę, šioje svetainėje net du kartus atskleidė tretiesiems asmenims prisijungimo prie jo paskyros duomenis, įskaitant bendrovės pareiškėjo telefono numeriu SMS žinute siųstą vienkartinį saugos kodą, skirtą prisijungti prie pareiškėjo sąskaitos, ir taip sudarė galimybę tretiesiems asmenims iš pareiškėjo sąskaitos atlikti ginčijamą mokėjimą. Pareiškėjas neigia spaudęs Nuorodą, Suklastotoje svetainėje ar kitur suvedęs prisijungimo prie savo paskyros duomenis ir (arba) kitaip juos atskleidęs tretiesiems asmenims ir teigia, kad tretieji asmenys įgijo prieigą prie pareiškėjo paskyros ir sąskaitos, taip pat iš šios sąskaitos atliko ginčijamą mokėjimą dėl nuo bendrovės priklausančių aplinkybių, susijusių su bendrovės vidaus sistemų saugumu.

Kaip matyti, ginčo šalys iš esmės nesutaria dėl aplinkybių, lėmusių tai, kaip tretieji asmenys galėjo prisijungti prie pareiškėjo sąskaitos ir iš jos atlikti ginčijamą mokėjimą, nors būtent šios aplinkybės ir turi esminės reikšmės vertinant, ar nagrinėjamo ginčo atveju bendrovei kyla pareiga gražinti pareiškėjui ginčijamo mokėjimo lėšas.

Pareiškėjas nurodė, kad jam priklauso *Iphone* įrenginys, kurį pareiškėjas įprastai naudoja sutartinių santykių su bendrove metu. Byloje neturima duomenų, kurie leistų nustatyti, kam priklauso *Android* įrenginys, iš kurio 2022 m. balandžio 13 d. buvo prisijungta prie pareiškėjo paskyros ir sąskaitos. Atsižvelgiant į tai, kad pareiškėjas nurodė nenaudojantis įrenginių, kuriuose būtų įdiegta *Android* programinė įranga, ir į tai, kad bendrovė nepateikė tai paneigiančių įrodymų ir nereiškė prieštaravimų pareiškėjo nurodytai informacijai, kad *Android* įrenginys priklauso ne jam, o tretiesiems asmenims, darytina išvada, kad abi ginčo šalys pripažįsta, kad *Android* įrenginys priklausė ir jį ginčijamo mokėjimo atlikimo dieną naudojo tretieji asmenys.

Ginčo byloje turimi duomenys leidžia teigti, kad prisijungimo prie pareiškėjo paskyros ir sąskaitos duomenys, įskaitant bendrovės SMS žinute pareiškėjui siųstą vienkartinį saugos kodą, skirtą prisijungti prie pareiškėjo sąskaitos, buvo žinomi ne tik pareiškėjui, bet ir tretiesiems asmenims. Kitaip tretieji asmenys nebūtų galėję prisijungti prie pareiškėjo paskyros ir sąskaitos ir iš jos atlikti ginčijamo mokėjimo.

Byloje nėra duomenų, kad nagrinėjamam ginčui aktualiu laikotarpiu į bendrovės vidaus sistemas būtų įsilaužta ir (arba) jas būtų paveikę techniniai trikdžiai, dėl kurių prisijungimo prie

pareiškėjo paskyros ir sąskaitos duomenys, įskaitant bendrovės pareiškėjui siųstų SMS žinučių turinį, galėjo tapti žinomi tretiesiems asmenims ir (arba) dėl kurių tretieji asmenys dėl nuo bendrovės priklausančių aplinkybių būtų kitaip įgiję neteisėtą prieigą prie pareiškėjo paskyros ir sąskaitos. Vadinasi, prisijungimo prie pareiškėjo paskyros ir sąskaitos duomenys tretiesiems asmenims, 2022 m. balandžio 13 d. prisijungusiems prie pareiškėjo paskyros ir sąskaitos, turėjo tapti žinomais kitu būdu.

Bendrovės teigimu, ginčijamo mokėjimo atlikimo aplinkybės, su jomis susijusių įvykių seka ir pobūdis bei laikotarpis, kuriuo buvo įvykdytas ginčijamas mokėjimas, sutampa su panašiu metu vykusiomis sukčiavimo atakomis, kurios buvo nukreiptos į bendrovės klientus. Bendrovės žiniomis, šios atakos metu neteisėtai veikiantys tretieji asmenys naudojo suklastotas interneto svetaines <https://paysera.cc/en/login> arba <https://paysera.ltd/en/login>, imituojančiomis bendrovės tikrąją interneto svetainę, kurioje dalis bendrovės klientų, nepastebėdami, kad bando jungtis prie savo paskyrų bendrovėje per suklastotas interneto svetaines, suklastotose interneto svetainėse suvedavo savo asmens bei personalizuotus prisijungimo prie bendrovėje turimų paskyrų ir mokėjimo sąskaitų duomenis, taip atskleisdami juos tretiesiems asmenimis, kurie gautus duomenis vėliau panaudojo prisijungti prie klientų paskyrų ir mokėjimo sąskaitų bei iš jų atlikti neautorizuotus mokėjimus.

Iš bylos duomenų matyti, kad pareiškėjas 2022 m. balandžio 9 d. 15 val. 24 m.¹ į savo telefono numerį gavo SMS žinutę², informuojančią apie gautą prašymą pateikti daugiau informacijos apie neseniai atliktą pavedimą, kurioje buvo pateikta Nuoroda, nukreipianti į Suklastotą svetainę. Suklastotos svetainės adresas sutampa su vienos iš sukčiavimo atakos metu sukčių naudotos suklastotos interneto svetainės adresu, t. y. <https://paysera.cc/en/login>. Nors ši SMS žinutė, remiantis pareiškėjo pateikta informacija, jo *Iphone* įrenginyje pateko į tą bendrą SMS žinučių, kurias pareiškėjui sutartinių santykių metu buvo siuntusi bendrovė, srautą, šią SMS žinutę pareiškėjui išsiuntė ne bendrovė. Byloje nėra duomenų, kurie leistų nustatyti, iš kokio mobiliojo telefono numerio pareiškėjui buvo siūsta minėta SMS žinutė su Nuoroda. Remiantis viešai prieinama informacija, išmaniuosiuose įrenginiuose gautos SMS žinutės yra dažnai grupuojamos pagal siuntėjo pavadinimą, o ne siuntėjo mobiliojo telefono numerį, tad tikėtina, kad pareiškėjo atveju būtent taip ir galėjo nutikti, kad sukčiaujantys tretieji asmenys, siūsdami pareiškėjui SMS žinutę su Nuoroda, save, kaip siuntėją, įvardijo neteisėtai pasinaudoję bendrovės pavadinimu, todėl pareiškėjo turimas *Iphone* įrenginys šių asmenų SMS žinutę priskyrė prie pareiškėjo anksčiau gautų SMS žinučių iš bendrovės.

Nors pareiškėjas neigia spaudęs šią Nuorodą, Suklastotoje svetainėje, į kurią nukreipia ši Nuoroda, ar kur kitur atskleidęs prisijungimo prie savo paskyros duomenis, iš bendrovės pateiktų vidaus sistemos duomenų matyti, kad 2022 m. balandžio 9 d. 15 val. 27 min., t. y. praėjus vos 3 minutėms po to, kai pareiškėjas į savo telefono numerį gavo SMS žinutę su Nuoroda, buvo prisijungta prie pareiškėjo paskyros ir toks jungimasis, kaip nurodė bendrovė, buvo inicijuotas iš Suklastotos svetainės. Nurodyto prisijungimo prie paskyros metu naudotas *Iphone* įrenginys, kuris priklauso pareiškėjui, tačiau iš kito IP adreso, negu pareiškėjas iki tol jungėsi, todėl bendrovė pareiškėjui jo el. paštu išsiuntė įspėjimą apie prisijungimą prie paskyros iš kito IP. Byloje nėra duomenų, kad pareiškėjas būtų praradęs jam priklausančią *Iphone* įrenginį ir (arba) kad aktualių laikotarpiu šis įrenginys būtų ne pareiškėjo žinioje. Atsižvelgiant į pirmiau nurodytas aplinkybes, darytina išvada, kad pareiškėjas vis dėlto lankėsi Suklastotoje svetainėje. Lietuvos bankas neturi galimybės nustatyti, koku tiksliai būdu pareiškėjas pateko į Suklastotą svetainę, tačiau, atsižvelgdamas į bendrovės pateiktą informaciją, kad iš Suklastotos svetainės inicijuotas prisijungimas prie pareiškėjo paskyros įvyko praėjus vos kelioms minutėms nuo to momento, kai pareiškėjas gavo SMS žinutę su Nuoroda į Suklastotą svetainę, Lietuvos bankas daro išvadą, kad labiausiai tikėtina, kad, priešingai, nei teigia pareiškėjas, jis vis dėlto paspaudė trečiųjų asmenų SMS žinute jam siūstą Nuorodą ir Suklastotoje svetainėje, galimai manydamas, kad jungiasi prie savo paskyros bendrovėje, suvedė savo prisijungimo prie paskyros duomenis, taip atskleisdamas juos Suklastotą svetainę valdantiems tretiesiems asmenims.

Iš tolesnės įvykių sekos matyti, kad praėjus keturioms dienoms, t. y. 2022 m. balandžio 13 d., tretieji asmenys 14 val. 32 min. 59 sek. inicijavo prisijungimo prie pareiškėjo paskyros slaptažodžio pakeitimą, po 3 sekundžių nuo slaptažodžio pakeitimo prisijungė prie pareiškėjo

¹ SMS žinutė Lietuvos laiku gauta 15 val. 24 min., pareiškėjo vietos laiku – 13 val. 24 m.

² Originalus gautos SMS žinutės turinys: „You have received a request to provide more information about your recent transfer <https://clk.one/h5Wt>“

paskyros ir po 13 sekundžių inicijavo prisijungimą prie pareiškėjo sąskaitos, bendrovė pareiškėjo telefono numeriu iš karto išsiuntė jam SMS žinutę su vienkartinio saugos kodu, skirtu prisijungti prie pareiškėjo sąskaitos, o po 30 sekundžių nuo tokio kodo išsiuntimo jis buvo suvestas pareiškėjo paskyroje ir taip tretieji asmenys prisijungė prie pareiškėjo sąskaitos, po 3 minučių atliko ginčijamą mokėjimą ir iš karto po jo atlikimo atsijungė nuo pareiškėjo paskyros.

Kaip matyti, tam, kad galėtų prisijungti prie pareiškėjo sąskaitos ir iš jos atlikti ginčijamą mokėjimą, tretieji asmenys turėjo ne tik iš anksto turėti prisijungimo prie pareiškėjo paskyros duomenis, bet ir gauti vienkartinį saugos kodą, kurį bendrovė realiuoju laiku, t. y. kai tretieji asmenys buvo prisijungę prie pareiškėjo paskyros, išsiuntė pareiškėjui SMS žinute į jo telefono numerį. Bendrovės nuomone, pareiškėjas suvedė SMS žinute gautą vienkartinį saugos kodą Suklastotoje svetainėje ir taip jį atskleidė tretiesiems asmenims. Byloje neturima duomenų, kurie tai patvirtintų arba paneigtų. Kadangi *Iphone* įrenginys tuo metu, kai bendrovė išsiuntė pareiškėjui SMS žinutę su vienkartinio saugos kodu, buvo pareiškėjo žinioje, darytina išvada, kad tretieji asmenys kitaip, negu iš paties pareiškėjo, nebūtų galėję sužinoti ir panaudoti šio kodo. Ginčo byloje nėra galimybės nustatyti, koku tiksliai būdu šis kodas galėjo būti perduotas tretiesiems asmenims, tačiau tai nekeičia fakto, kad jis buvo perduotas, nes tretieji asmenys jį panaudojo ir taip gavo prieigą prie pareiškėjo sąskaitos.

Esant tokiai situacijai, kai byloje turimų duomenų visuma leidžia daryti išvadą, kad pareiškėjas galimai atskleidė tretiesiems asmenims prisijungimo prie savo paskyros ir sąskaitos duomenis, bet pareiškėjas neigia atlikęs bet kokius veiksmus, dėl kurių galėjo prarasti šiuos duomenis, įvertinti konkrečių pareiškėjo, kaip mokėtojo, veiksmų atsargumo laipsnį yra neįmanoma arba įmanoma apie jo veiksmus darant tik labiausiai tikėtinas prielaidas. Įrodymų pakankamumo taisyklė civiliniame procese grindžiama vadinamąja tikėtinumo taisykle (tikimybių pusiausvyros principu). Kasacinio teismo jurisprudencijoje ne kartą pažymėta, kad įrodinėjimas civiliniame procese turi savo specifiką, – nenustatyta, kad išvadą apie tam tikrų faktų buvimą galima daryti tik tada, kai dėl jų egzistavimo absoliučiai nėra abejonių; išvadą apie faktų buvimą teismas civiliniame procese gali daryti ir tada, kai tam tikros abejonės dėl fakto buvimo išlieka, tačiau byloje esančių įrodymų visuma leidžia manyti esant labiau tikėtina atitinkamą faktą buvus, nei jo nebuvus³.

Neatsargumo laipsnio vertinimas yra susijęs su ginčo byloje nustatytų individualių, specifinių aplinkybių, kurias patvirtina ginčo byloje esantys įrodymai ir (arba) yra šalių neginčijamos neautorizuotos mokėjimo operacijos įvykdymo aplinkybės, visumos vertinimu. 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).

Kaip ir buvo minėta pirmiau, iš ginčo byloje turimų duomenų galima teigti, kad, priešingai, nei teigia pareiškėjas, labiau tikėtina, kad pareiškėjas vis dėlto pats atskleidė tretiesiems asmenims prisijungimo prie savo paskyros ir sąskaitos duomenis, įskaitant SMS žinute gautą vienkartinį saugos kodą. Nors pareiškėjas taip pat neigė spaudęs jam 2022 m. balandžio 9 d. trečiųjų asmenų siūstoje SMS žinutėje pateiktą Nuorodą, byloje turimi duomenys leidžia daryti išvadą, kad jis šią nuorodą buvo paspaudęs. Vertinant SMS žinutės su Nuoroda turinį ir faktą, kad ši žinutė buvo įterpta į bendrą tikrų pareiškėjo iš bendrovės gautų SMS žinučių srautą, manytina, kad pareiškėjui objektyviai galėjo atrodyti, kad SMS žinutę su

³ Lietuvos Aukščiausiojo Teismo Civilinių bylų skyriaus teisėjų kolegijos 2008 m. rugpjūčio 25 d. nutartis civilinėje byloje Nr. 3K-3-304/2008; 2009 m. kovo 16 d. nutartis civilinėje byloje Nr. 3K-3-101/2009 ir kt.

Nuoroda jam galėjo atsiųsti bendrovė. Tačiau, atsižvelgiant į tai, kad šioje SMS žinutėje buvo prašoma pateikti papildomą informaciją apie mokėjimą, kurio pareiškėjas tuo metu neinicijavo, ir į tai, kad iki šios SMS žinutės gavimo bendrovė nebuvo prašiusi pareiškėjo teikti informacijos tokiu būdu ir forma, t. y. per SMS žinutę atsiųstą Nuorodą, manytina, kad pareiškėjas vis dėlto turėjo kritiškai vertinti šios SMS turinį ir susilaikyti nuo bet kokių veiksmų, kol nepasitikrino šios informacijos sutartinių santykių su bendrove pareiškėjui įprastais prieinamais būdais (pvz., patikrinti savo sąskaitos išrašą per mobiliąją programėlę, pasitikrinti savo el. paštą, susisiekti su bendrove ir pan.).

Net jei per Nuorodą patekęs į Suklastotą svetainę pareiškėjas neatkreipė dėmesio į tai, kad rodomas Suklastotos svetainės adresas nesutampa su bendrovės tikrosios interneto svetainės adresu ir (arba) Suklastotos svetainės turinys skiriasi nuo tikrojoje bendrovės svetainėje įprastai pateikiama informacija, manytina, kad pareiškėjui turėjo kilti įtarimų, kad SMS žinutėje nurodyta informacija nepasitvirtino, t. y. kad nereikėjo bendrovei pateikti informacijos apie joki paskutinį pervedimą, kurį, remiantis šia SMS žinute, jis tariamai atliko. Byloje neturima duomenų, kad pareiškėjas po šios SMS žinutės gavimo būtų kreipėsis į bendrovę ir bandęs išsiaiškinti jos siuntimo ir (ar) turinio aplinkybes.

Vertinant pareiškėjo elgesį 2022 m. balandžio 13 d., kai tretieji asmenys prisijungė prie pareiškėjo paskyros ir sąskaitos, svarbu pažymėti, kad pareiškėjas, nors pats tuo metu ir nesinaudojo savo paskyra, į savo telefono numerį gavo net dvi SMS žinutes, kurios turėjo sukelti jam įtarimų, t. y. SMS žinutę dėl slaptažodžio pakeitimo iš įrenginio, kuris priklauso ne jam, ir SMS žinutę su vienkartinio patvirtinimo kodu, skirtu prisijungti prie pareiškėjo sąskaitos. Tačiau byloje turimi duomenys leidžia daryti išvadą, kad pareiškėjas ne tik kad nevertino šių SMS žinučių kritiškai ir iš karto nebandė susisiekti su bendrove dėl jų, bet ir gautą vienkartinį saugos kodą, skirtą prisijungti prie pareiškėjo sąskaitos, perdavė tretiesiems asmenims, kurie, panaudodami jį, prisijungė prie pareiškėjo sąskaitos ir iš jos atliko ginčijamą mokėjimą.

Atkreiptinas dėmesys, kad, vadovaujantis pareiškėjo ir bendrovės sudarytos Sutarties 13.4 papunkčiu, pareiškėjas buvo įsipareigojęs 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 pareiškėjo vardu. Šiame papunktyje taip pat nustatyta, kad jei pareiškėjas nesilaikė prieš tai nurodyto įsipareigojimo ir (arba) galėjo, bet neužkirto tam kelio ir (arba) tokius veiksmus atliko tyčia ar dėl didelio savo neatsargumo, jis visa apimtimi prisiima dėl to patirtus nuostolius bei įsipareigoja atlyginti kitų asmenų nuostolius, jei jie buvo patirti dėl pareiškėjo nurodytų veiksmų ar neveikimo. Pagal Sutarties „Mokėjimo priemonių“ priedo sąlygų 8 punktą, šalys buvo susitarusios, kad pareiškėjui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai, jei mokėtojas juos patyrė veikdamas nesąžiningai arba dėl didelio neatsargumo ar tyčios neįvykdęs vienos ar kelių šiame Sutartyje nustatytų pareigų, neapsaugojęs mokėjimo priemonės ar jos slaptažodžių ir (arba) naudojėsis mokėjimo priemone ne pagal nustatytas taisykles, taip pat atvejais, kai neautorizuotos operacijos atliktos naudojant slaptažodžius. Remiantis Sutartyje pateiktų sąvokų aprašymais, pareiškėjo ir bendrovės santykiuose slaptažodžiu laikomas „bet koks Sistemoje sukurtas Kliento kodas, Saugesnio autentiškumo patvirtinimo procedūros metu naudojamas Sistemoje sukurtas Kliento kodas ar Paysera Klientui pateiktas kodas, skirtas priėjimui prie Paskyros ir (arba) Paysera Sąskaitos ar atskiros Paysera teikiamos paslaugos inicijavimui, patvirtinimui ir (arba) valdymui, Mokėjimo operacijos inicijavimui, autorizavimui, vykdymui, tvirtinimui ar gavimui“.

Ginčo byloje nėra duomenų, kad pareiškėjas buvo tinkamai nesupažindintas su Sutarties sąlygomis ar kad jų nesuprato. Taigi, pareiškėjas iš esmės turėjo suprasti, kad prisijungimo prie paskyros ir sąskaitos duomenų, įskaitant SMS žinute gautą vienkartinį saugos kodą, suvedimas yra skirtas prisijungimui prie pareiškėjo paskyros ir sąskaitos patvirtinti ir kad šių duomenų naudojimas, neprisijungus prie paskyros ir (ar) neturint tikslo joje atlikti kitų veiksmų, gali sukelti neigiamas pasekmes, įskaitant neautorizuotų mokėjimo operacijų iš sąskaitos įvykdymą.

Lietuvos banko nuomone, jeigu pareiškėjas būtų buvęs pakankamai atidus ir rūpestingas nagrinėjamoje situacijoje, būtų galėjęs pastebėti trečiųjų asmenų neteisėtus veiksmus ir, labai tikėtina, būtų išvengęs iš jo sąskaitos atlikto ginčijamo mokėjimo. Byloje turimi duomenys, įskaitant žinomą aktualių įvykių seką, leidžia daryti išvadą, kad nagrinėjamu atveju pareiškėjo elgesys gali būti pripažintas kaip elgesys, iš esmės besiskiriantis nuo atsargaus elgesio reikalavimų, jis galiausiai lėmė tai, kad pareiškėjas pats suteikė tretiesiems asmenims prieigą prie jo paskyros ir sąskaitos ir taip sudarė šiems asmenims galimybę pareiškėjo vardu iš jo

sąskaitos atlikti ginčijamą mokėjimą.

Mokėjimų įstatymo 34 straipsnyje reglamentuojamos mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigos: 1) naudotis mokėjimo priemone pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas; 2) sužinojus apie mokėjimo priemonės praradimą, vagystę arba neteisėtą pasisavinimą ar neautorizuotą jos naudojimą, nedelsiant apie tai pranešti mokėjimo paslaugų teikėjui arba jo nurodytam subjektui. Mokėjimo paslaugų vartotojas, gavęs mokėjimo priemonę, privalo imtis veiksmų, kad būtų apsaugoti personalizuoti saugumo duomenys (2 dalis). Taigi, įvertinus ginčo byloje turimus duomenis bei ginčo šalių paaiškinimus apie ginčijamo mokėjimo atlikimo aplinkybes, galima teigti, kad pareiškėjas savo mokėjimo priemone, t. y. paskyra, per kurią pareiškėjas galėjo nuotoliniu būdu naudotis savo sąskaita, naudojosi nesilaikydamas mokėjimo priemonės išdavimą ir naudojimą reglamentuojančių sąlygų ir neįvykdė Mokėjimų įstatymo 34 straipsnyje jam nustatytų pareigų.

Lietuvos banko nuomone, įvertinus pirmiau išdėstytas ginčo byloje nustatytas aplinkybes ir padarytas išvadas, galima teigti, kad pareiškėjas iki ginčijamo mokėjimo įvykdymo galėjo pastebėti tik jam žinomų mokėjimo priemonės duomenų praradimą ir neautorizuotą mokėjimo priemonės naudojimą, t. y. kad pareiškėjo paskyra ir sąskaita naudojasi tretieji asmenys. Mokėjimų įstatymo 39 straipsnio 3 dalyje nustatyta, kad mokėtoju 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. Kaip ir buvo minėta, Lietuvos banko nuomone, nagrinėjamo ginčo atveju pareiškėjo elgesys, dėl kurio jis prarado savo mokėjimo priemonės duomenis, taip sudarydamas galimybę tretiesiems asmenims iš pareiškėjo sąskaitos atlikti ginčijamą mokėjimą, gali būti laikomas itin neatsargiu. Įvertinus pirmiau išdėstytą informaciją, konstatuotina, kad yra pagrindas pareiškėjui taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, todėl pareiškėjo reikalavimas bendrovei grąžinti neautorizuotų mokėjimo operacijų lėšų sumą yra nepagrįstas ir 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 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