LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

SPRENDIMAS DĖL X.X. IR AB SEB BANKO GINČO NAGRINĖJIMO

2022-05-11 Nr. 429-170
Vilnius

Lietuvos bankas gavo X.X. (toliau – pareiškėjos atstovė) kreipimąsi, kuriuo prašoma išnagrinėti tarp X.X. (toliau – pareiškėja) ir AB SEB banko (toliau – bankas) kilusį ginčą.

N u s t a t y t a:

2021 m. spalio 3 d. 19 val. 22 min. iš pareiškėjos sąskaitos banke Nr. *duomenys neskelbiami* buvo inicijuota 3 400 Eur mokėjimo operacija ir 19 val. 24 min. iš pareiškėjos sąskaitos banke Nr. *duomenys neskelbiami* buvo inicijuota 530 Eur mokėjimo operacija (toliau – mokėjimo operacijos), bendra mokėjimo operacijų suma – 3 930 Eur, lėšos pervestos lėšų gavėjui Oluwadarai Olaniyanui Collinsui (Oluwadara Olaniyan Collins) (toliau – gavėjas).

2021 m. spalio 5 d. pareiškėja telefonu kreipėsi į banką ir informavo, kad iš jos banko sąskaitų be jos žinios ir sutikimo yra įvykdytos mokėjimo operacijos. Pareiškėja banko darbuotojai teigė, kad 2021 m. spalio 3 d. į savo telefoną gavo SMS žinutę, kurioje buvo pranešama, kad pareiškėjos paskyra yra užblokuota, ir buvo prašoma paspausti SMS žinutėje pateiktą aktyvią nuorodą, tačiau pareiškėja teigė, kad šią SMS žinutę pamatė tik 2021 m. spalio 5 d. ir SMS žinutėje pateiktos nuorodos nespaudė. Banko darbuotojai pareiškėja teigė, kad 2021 m. spalio 3 d. jokių mokėjimo operacijų iš savo banko sąskaitos nevykdė, nesinaudojo savo mobiliuoju telefonu, įskaitant „Smart-ID" programėlę, ir niekam nebuvo nei perdavusi, nei atskleidusi savo personalizuotų saugos duomenų, todėl nežino, kaip iš jos banko sąskaitos be jos žinios ir sutikimo galėjo būti įvykdytos mokėjimo operacijos. Pareiškėja taip pat teigė, kad iš banko gavo SMS žinutę, kurioje buvo informuota apie jos vardu sukurtą naują „Smart-ID" paskyrą, tačiau tvirtino, kad šią žinutę pamatė tik 2021 m. spalio 5 d.

Atlikęs tyrimą bankas nustatė, kad 2021 m. spalio 3 d. 17 val. 42 min. pareiškėja į savo mobilųjį telefoną Nr. *duomenys neskelbiami* iš trečiųjų asmenų gavo SMS žinutę su tokiu tekstu: *„SEB" programa uzblokuota del saugumo. Noredami to isvengti, spustelekite nuoroda: HK38721.com."* Banko nuomone, nors pareiškėja tai neigia, tačiau tikėtina, kad ji paspaudė aktyvią nuorodą ir pateko į trečiųjų asmenų suklastotą banko interneto puslapį, jame suvedė savo banko atpažinimo kodą ir asmens kodą, o savo mobiliajame įrenginyje į savo „Smart-ID" paskyrą suvedė „Smart-ID" PIN1 ir PIN2 kodus. Tokie pareiškėjos veiksmai lėmė tai, kad tretieji asmenys pasisavino pareiškėjos personalizuotus saugos duomenis ir 2021 m. spalio 3 d. 19 val. 17 min. savo įrenginyje, kuris nepriklauso pareiškėjai, pareiškėjos vardu susikūrė kitą „Smart-ID" paskyrą. Taip tretieji asmenys įgijo galimybę pareiškėjos vardu prie pareiškėjos interneto banko ir kartu sąskaitos jungtis iš kito įrenginio ir pareiškėjos vardu inicijuoti, tvirtinti veiksmus ir operacijas (tvirtinti mokėjimus, atidaryti sąskaitas, keisti operacijų limitus, peržiūrėti likučius, sudaryti sutartis, teikti prašymus ir pan.).

2021 m. spalio 3 d. 19 val. 15 min. bankas SMS žinute pareiškėjos telefono numeriu informavo pareiškėją apie jos vardu sukurtą naują „Smart-ID" paskyrą: *„Gerb. Kliente, Jūsų vardu SEB banke registruojama „Smart-ID Basic" paskyra. Jei to neinicijavote, prašom kuo skubiau susisiekti tel. +370 5 268 2800. SEB bankas."*

2021 m. spalio 3 d. 19 val. 18 min. tretieji asmenys pasinaudodami naujai sukurta „Smart-ID" paskyra prisijungė prie pareiškėjos interneto banko ir pareiškėjos vardu naudodamiesi naujai sukurta „Smart-ID" paskyra inicijavo mokėjimo operacijas.

Išnagrinėjęs pareiškėjos prašymą grąžinti neautorizuotų mokėjimo operacijų lėšas, bankas pareiškėjai pateikė atsakymą, kad bankas pareiškėjai negrąžins mokėjimo operacijų lėšų.

Nesutikdama su banko atsakymu, pareiškėja kreipėsi į Lietuvos banką dėl ginčo nagrinėjimo. Kreipimesi į Lietuvos banką pareiškėjos atstovė paaiškino, kad pareiškėja, 2021 m. spalio 5 d. ketindama atlikti periodinius atsiskaitymo mokėjimus, pastebėjo, kad iš jos banko sąskaitų be jos žinios ir sutikimo yra įvykdytos mokėjimo operacijos, kurių pati pareiškėja neinicijavo. Pareiškėjos atstovė taip pat teigė, kad pareiškėja jokiems tretiesiems asmenims nebuvo perdavusi ar kitaip atskleidusi savo personalizuotų saugos duomenų – jie buvo žinomi tik pačiai pareiškėjai. Pareiškėjos atstovės teigimu, pareiškėja nespaudė jokių aktyvių nuorodų, nukreipiančių į banko interneto puslapį.

Pareiškėjos atstovės nuomone, bankas atsako už klientų piniginių lėšų jų sąskaitose saugumą, įskaitant banko sistemų saugumą bei tinkamą mokėjimo operacijų autorizavimą, ir turi užtikrinti, kad būtų įvykdytos tik tos mokėjimo operacijos, kurios yra tinkamai autorizuotos. Vis dėlto įvykdytos mokėjimo operacijos buvo pareiškėjos neautorizuotos, taip pat nėra jokių duomenų apie pareiškėjos tyčią ar nesąžiningumą, taip pat nėra jokių įrodymų, kad pareiškėja atliko banko tyrimo metu nustatytus tikėtinus pareiškėjos veiksmus, lėmusius pareiškėjos neautorizuotas mokėjimo operacijas, todėl, pareiškėjos atstovės nuomone, bankas turėtų pareiškėjai grąžinti mokėjimo operacijų lėšas.

Bankas nesutinka tenkinti pareiškėjos reikalavimo. Atsiliepime bankas nurodė tyrimo metu nustatytas mokėjimo operacijų inicijavimo ir vykdymo aplinkybes, tačiau pareiškėja nesutinka su banko pateikta informacija ir teigia, kad SMS žinute gautos aktyvios nuorodos nespaudė, mokėjimo operacijų inicijavimo dieną nesinaudojo savo interneto banku, neinicijavo jokių mokėjimo operacijų ir nesinaudojo savo mobiliuoju telefonu, todėl tiek trečiųjų asmenų atsiųstą SMS žinutę, tiek banko atsiųstą SMS žinutę apie naujos „Smart-ID" paskyros sukūrimą pamatė tik 2021 m. spalio 5 d. Atsiliepime bankas pažymėjo, kad su tokiais pareiškėjos teiginiais negali sutikti, nes banko vidinių sistemų išrašai nepatvirtina pareiškėjos teiginių.

Bankas teigia, kad pareiškėja SMS žinutę iš trečiųjų asmenų su prašymu paspausti aktyvią nuorodą gavo anksčiau (17 val. 42 min.) nei banko siųstą SMS žinutę (19 val. 15 min.) su pranešimu apie naujos „Smart-ID" paskyros sukūrimą, banko vidinių sistemų duomenys įrodo, kad naujos „Smart-ID" paskyros sukūrimas buvo patvirtintas suvedus „Smart-ID" PIN1 ir PIN2 kodus. Taigi, banko teigimu, yra nepagrįstas pareiškėjos teiginys, kad mokėjimo operacijos įvykdytos be pareiškėjos veiksmų.

Bankas teigė nesutinkantis ir su pareiškėjos teiginiais, kad ji galėjo nepastebėti SMS žinutės su aktyvia nuoroda, kurią jai siuntė tretieji asmenys, kad nespaudė aktyvios nuorodos, nesuvedė savo personalizuotų saugos duomenų, nepastebėjo banko SMS žinutės apie naujos „Smart-ID" paskyros sukūrimą. Bankas atkreipė dėmesį, kad pareiškėja nepateikia jokių duomenų apie savo atliktus veiksmus.

Bankas paaiškino, kad, pareiškėjos vardu trečiųjų asmenų naudojamame įrenginyje sukūrus „Smart-ID" paskyrą, mokėjimo operacijos buvo inicijuotos iš kito IP adreso, kuris nepriklauso pareiškėjai. Vis dėlto IP adreso neatitikimas nepaneigia fakto, kad mokėjimo operacijos buvo inicijuotos ir patvirtintos dėl pareiškėjos iniciatyva atliktų veiksmų – tikėtina, pareiškėjai paspaudus trečiųjų asmenų atsiųstą aktyvią nuorodą ir atskleidus personalizuotus prisijungimo prie interneto banko paskyros duomenis (atpažinimo kodą, asmens kodą ir tik pareiškėjai žinomus „Smart-ID" paskyros PIN1 ir PIN2 kodus).

Banko teigimu, pareiškėjos veiksmuose, dėl kurių ji prarado savo mokėjimo priemonę, buvo didelio neatsargumo požymių. Pareiškėja dėl savo didelio neatsargumo neįgyvendino Lietuvos Respublikos mokėjimų įstatymo 34 straipsnyje aptartų mokėjimo paslaugų vartotojo pareigų, susijusių su naudojimusi mokėjimo priemone ir personalizuotais saugumo duomenimis, neišsaugojo personalizuotų saugos duomenų, tai lėmė, kad pareiškėja prarado mokėjimo priemonę, o tretieji asmenys įgijo galimybę pareiškėjos vardu inicijuoti mokėjimo operacijas. Pareiškėja nesilaikė ir banko Bendrųjų paslaugų teikimo taisyklių (toliau – Taisyklės) 1 priedo 10 skyriuje nustatytų reikalavimų saugoti banko suteiktą mokėjimo priemonę ir su ja susijusius personalizuotus saugumo duomenis bei imtis visų reikiamų veiksmų, kad personalizuoti saugumo duomenys nebūtų atskleisti kitiems asmenims. Taip pat pareiškėja nesilaikė ir banko Paslaugų interneto banke teikimo sąlygų aprašo (toliau – Aprašas) 20.4.4 papunktyje ir 38^5 punkte nustatytų mokėjimo priemonės savininko pareigų: saugoti atpažinimo priemones, nedelsiant informuoti banką apie šių priemonių praradimą ar slaptumo pažeidimą, laikyti paslaptyje banko atpažinimo kodą, slaptažodžius, PIN kodus, neužrašyti jų ant generatoriaus ar kitų kartu su juo laikomų daiktų ir jokia kita forma neatskleisti ar nepadaryti jų prieinamų tretiesiems asmenims.

Bankas teigia, kad įvertinęs pareiškėjos elgesį mano, kad pareiškėja elgėsi itin neapdairiai

ir neatsargiai: paspaudė neaiškią nuorodą, suvedė savo interneto banko atpažinimo kodą, asmens kodą ir savo mobiliajame įrenginyje savo atliekamus veiksmus patvirtino suvesdama tik jai žinomus, jos žinioje esančios „Smart-ID" paskyros PIN1 ir PIN2 kodus, dėl to yra pagrindas pareiškėjai taikyti Mokėjimų įstatymo 39 straipsnio 3 dalies nuostatą, 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.

Bankas pažymėjo, kad pareiškėja galėjo lengvai suprasti ir įvertinti savo atliekamų veiksmų reikšmę ir pasekmes, nes tokius veiksmus atliko ne pirmą kartą – „Smart-ID" programėle, kaip atpažinimo priemone, naudojasi nuo 2020 metų, daug kartų yra jungusis prie interneto banko, tvirtinusi mokėjimo nurodymus, todėl turėjo nesunkiai suprasti, kad interneto banko atpažinimo kodas, asmens kodas ir „Smart-ID" PIN1 ir PIN2 kodai yra naudojami jungtis prie interneto banko, mokėjimo nurodymams tvirtinti, kitiems veiksmams interneto banke atlikti, ir turėjo kritiškai įvertinti minėtų duomenų suvedimą, nes žinojo, kad pati mokėjimo operacijų neinicijavo.

Bankas taip pat atkreipė dėmesį į tai, kad pareiškėja nesilaikė ne tik Mokėjimų įstatymo, Taisyklių ir Aprašo reikalavimų, susijusių su mokėjimo priemonės naudojimu ir personalizuotų saugos duomenų saugojimu, bet nesilaikė ir „Smart-ID" leidėjo *SK ID solutions AS* (toliau – SK) „Q Smart-ID" sertifikatų naudojimo sąlygose (toliau – Sąlygos) nustatytų „Smart-ID" naudojimo reikalavimų, todėl tretieji asmenys pasisavino pareiškėjos tapatybę. Minėtų Sąlygų 5.2 papunktyje nustatytos „Smart-ID" vartotojo pareigos: 5.2.3. laikytis SK nustatytų reikalavimų; 5.2.6. naudoti jo / jos privatųjį raktą ir sertifikatą remiantis nuostatomis ir sąlygomis, įskaitant 10 skirsnyje ir Estijos Respublikos ir Europos Sąjungos teisės aktuose išdėstytus taikytinus susitarimus; 5.2.8. užtikrinti, kad vartotojo privatųjį raktą naudotų ir valdytų tik jis. Be to, SK savo interneto svetainėje papildomai paprasta ir patogia forma pateikia informaciją „Smart-ID" vartotojams apie naudojimąsi „Smart-ID" priemone. „Skiltyje „PIN kodai ir sauga" atkreipiamas vartotojų dėmesys į PIN kodų neatskleidimą. Skiltyje „Ar naudotis „Smart-ID" yra saugu?" sakoma, kad PIN1 ir PIN2 kodai yra slapti ir juos žino tik vartotojas. Taip pat nurodyti „Smart-ID" saugaus naudojimo principai: „niekada neatskleiskite savo PIN1 ir PIN2 kodų kitiems", „visada įsitikinkite, jog vykdoma būtent jūsų iškviesta „Smart-ID" operacija". Skiltyje „Kaip užtikrinti išmaniojo įrenginio ir „Smart-ID" apsaugą?" pateikiama išsamesnė informacija, kaip „Smart-ID" vartotojas turi laikytis Sąlygose nustatytų reikalavimų (pvz., PIN1 ir PIN2 kodų neatskleidimo ir pan.): „<...> Reaguokite tik tada, jei veiksmą inicijavote jūs pats! Jei operaciją inicijavote ne jūs, niekada neįveskite PIN kodų! Ekrane pamatę atsitiktinę tapatybės nustatymo užklausą, ignoruokite ją. Jei tai nutiktų dar kartą, prašome susisiekti su mūsų klientų aptarnavimo skyriumi ir mes paaiškinsime, ką reikėtų daryti tokiu atveju."

Atsiliepime bankas prašo atmesti pareiškėjos reikalavimą kaip nepagrįstą.

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

Vadovaujantis Lietuvos banko valdybos 2012 m. sausio 26 d. nutarimu Nr. 03-23 patvirtintų Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių 45 punktu, vartojimo ginčai Lietuvos banke nagrinėjami laikantis rungimosi, ginčų nagrinėjimo operatyvumo, koncentracijos, ekonomiškumo ir bendradarbiavimo principų. Vartotojas ir finansų rinkos dalyvis privalo įrodyti tas aplinkybes, kuriomis remiasi kaip savo reikalavimų arba atsikirtimų pagrindu, išskyrus atvejus, kai remiamasi aplinkybėmis, kurių nereikia įrodinėti. Lietuvos bankas ginčo nagrinėjimo proceso metu neatlieka Lietuvos Respublikos Lietuvos banko įstatymo 42^1 straipsnyje reglamentuotų patikrinimų, skirtų faktinėms aplinkybėms, susijusioms su Lietuvos banko priežiūrimo finansų rinkos dalyvio galimu Lietuvos banko kompetencijai priskirtų teisės aktų reikalavimų pažeidimu, nustatyti ir įvertinti. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Pareiškėjos ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjai jos vardu banke atidarytose sąskaitose atliktų mokėjimo operacijų lėšas, iš viso – 3 930 Eur. Pareiškėja teigia neautorizavusi mokėjimo operacijų, neigia trečiųjų asmenų suklastotame banko interneto puslapyje suvedusi savo prisijungimo prie banko paskyros duomenis ir savo mobiliajame telefone suvedusi „Smart-ID" PIN1 ir PIN2 kodus. Pareiškėja neneigė į savo mobilųjį telefoną iš trečiųjų asmenų gavusi SMS žinutę su aktyvia nuoroda, tačiau teigė, kad jos nespaudė ir kad niekas kitas negalėjo žinoti jos personalizuotų prisijungimo prie banko sąskaitos duomenų, įskaitant „Smart-ID" PIN1 ir PIN2 kodus. Pareiškėjos teigimu,

tretieji asmenys be jos žinios ir sutikimo įgijo galimybę iš jos banko sąskaitos įvykdyti mokėjimo operacijas, nes bankas neužtikrino mokėjimo sistemų saugumo ir įvykdė neautorizuotas mokėjimo operacijas.

Bankas teigia, kad pareiškėjos mokėjimo operacijos buvo patvirtintos šalių sutarta forma ir tvarka, dėl to bankas jas pagrįstai įvykdė. Taip pat bankas teigia, kad yra sąlygos pareiškėjos elgesį, prarandant savo mokėjimo priemonę, vertinti kaip labai neatsargų, todėl bankas mano, kad neturi pareigos kompensuoti pareiškėjai jos patirtų nuostolių dėl mokėjimo operacijų įvykdymo. Dėl šių priežasčių, banko nuomone, visi mokėjimo operacijų nuostoliai turėtų tekti pareiškėjai.

Tarp šalių nėra ginčo, kad pareiškėjos sutikimas, kad mokėjimo operacijos būtų vykdomos, nebuvo duotas, t. y. tiek pareiškėja, tiek bankas pripažįsta, kad mokėjimo operacijas inicijavo ne pati pareiškėja, bet tretieji asmenys, kurie buvo įgiję galimybę naudotis pareiškėjos mokėjimo priemonė kaip sava. Atsiliepime bankas iš esmės remiasi Mokėjimų įstatymo nuostatomis, reglamentuojančiomis mokėtojo atsakomybę už neautorizuotas mokėjimo operacijas. Taigi, galima daryti išvadą, kad bankas pripažįsta, kad mokėjimo operacijos nagrinėjamo ginčo atveju laikytinos neautorizuotomis. Taip pat svarbu tai, kad ginčo byloje banko pateikti vidaus sistemų duomenys apie mokėjimo operacijų įvykdymą leidžia teigti, kad mokėjimo operacijos buvo patvirtintos šalių sutarta forma ir tvarka, tačiau inicijuotos ne pačios pareiškėjos, bet trečiųjų asmenų. Atsižvelgiant į tai, kad iš esmės abi ginčo šalys sutaria, kad mokėjimo operacijos galėjo būti inicijuotos be pareiškėjos žinios ir sutikimo, bei į tai, kad ginčo byloje turimi banko sistemų duomenys leidžia teigti, kad mokėjimo operacijas inicijavo ne pati pareiškėja, toliau sprendime nebus analizuojamos su mokėjimo operacijų autorizavimo vertinimu susijusios aplinkybės, o mokėjimo operacijos laikomos pareiškėjos neautorizuotomis.

Ginčo šalys iš esmės nesutaria dėl aplinkybių, lėmusių tai, tretieji asmenys galėjo įgyti pareiškėjos mokėjimo priemonę ir ja naudotis kaip sava, t. y. iš pareiškėjos banko sąskaitos inicijuoti mokėjimo operacijas. Šiame kontekste pažymėtina, kad pareiškėjos pateikti paaiškinimai apie mokėjimo operacijų įvykdymo aplinkybes nesutampa su banko vidinių sistemų užfiksuotais duomenimis. Pareiškėja kategoriškai neigia spaudusi jai SMS žinute atsiųstą aktyvią nuorodą, taip pat neigia atidarytoje nuorodoje vedusi savo banko atpažinimo kodą ir asmens kodą, o savo mobiliajame telefone suvedusi Smart-ID" PIN1 ir PIN2 kodus. Be to, pareiškėja teigia, kad jos personalizuoti prisijungimo prie interneto banko duomenys, įskaitant „Smart-ID" PIN1 ir PIN2 kodus, buvo žinomi tik jai ir niekam kitam ji jų nebuvo nei perdavusi, nei atskleidusi. Vis dėlto banko pateikti vidinių sistemų išrašai patvirtina, kad mokėjimo operacijos buvo inicijuotos iš kito, pareiškėjai nepriklausančio IP adreso, panaudojus tik pareiškėjai žinomus personalizuotus saugos duomenis ir sukūrus naują „Smart-ID" paskyrą kitame, ne pareiškėjai priklausančiame, mobiliajame įrenginyje. Taigi, ginčo byloje turimi duomenys leidžia teigti, kad pareiškėjos personalizuoti prisijungimo prie banko sąskaitos duomenys, įskaitant „Smart-ID" PIN1 ir PIN2 kodus, buvo žinomi ne tik pareiškėjai, bet ir tretiesiems asmenims. Vadinasi, tretiesiems asmenims kažkokiu būdu turėjo būti atskleisti tik pareiškėjai žinomi personalizuoti saugos duomenys.

Kadangi pareiškėja kategoriškai neigia spaudusi jai SMS žinute atsiųstą aktyvią nuorodą ir iš esmės nesutampa pareiškėjos pateikti paaiškinimai apie mokėjimo priemonės praradimo aplinkybes su banko sistemų užfiksuotais duomenimis, nėra galimybės neabejotinai teigti, kad pareiškėja mokėjimo priemonę prarado dėl neteisėtų trečiųjų asmenų veiksmų, t. y. iš esmės nėra aišku, kaip tretieji asmenys galėjo įgyti pareiškėjos mokėjimo priemonę ir ja naudotis kaip sava.

Nagrinėjamo ginčo atveju ginčo šalys nesutaria ir dėl to, kam turėtų tekti atsakomybė už neautorizuotų mokėjimo operacijų įvykdymą: bankas teigia, kad pareiškėjos elgesys, tretiesiems asmenims atskleidžiant savo personalizuotus saugos duomenis ir prarandat savo mokėjimo priemonę, buvo labai neatsargus, tai lėmė neautorizuotų mokėjimo operacijų iš pareiškėjos sąskaitos įvykdymą, pareiškėja teigia lėšas praradusi dėl banko mokėjimų sistemos saugumo trūkumų ir neigia tretiesiems asmenims galėjusi atskleisti ar perduoti savo personalizuotus saugos duomenis.

Siekiant išspręsti tarp pareiškėjos ir banko kilusį ginčą, Lietuvos banko vertinimu, būtina nustatyti, ar bankas turėjo (turi) pareigą grąžinti pareiškėjai neautorizuotų mokėjimo operacijų sumas.

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.

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

Pagal Mokėjimų įstatymo 39 straipsnio 1 dalį, mokėtojui gali tekti dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai iki 50 eurų, kai šie nuostoliai patirti dėl: 1) prarastos ar pavogtos mokėjimo priemonės panaudojimo; 2) neteisėto mokėjimo priemonės pasisavinimo. Tačiau, kaip nustatyta Mokėjimų įstatymo 39 straipsnio 2 dalyje, mokėtojas neturi patirti jokių nuostolių, jeigu jis iki mokėjimo operacijos įvykdymo negalėjo pastebėti mokėjimo priemonės praradimo, vagystės arba neteisėto pasisavinimo, išskyrus atvejus, kai jis veikė nesąžiningai (1 punktas). Mokėjimų įstatymo 39 straipsnio 3 dalyje nustatyta, kad mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai, jeigu jis juos patyrė veikdamas nesąžiningai arba tyčia ar dėl didelio neatsargumo neįvykdęs vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų. Tokiais atvejais Mokėjimų įstatymo 39 straipsnio 1 dalyje nustatytas didžiausios nuostolių sumos ribojimas netaikomas.

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

Bankas teigia, kad tretieji asmenys neteisėtu būdu galėjo pasisavinti pareiškėjos prisijungimo prie banko paskyros duomenis tik todėl, kad pareiškėja dėl savo didelio neatsargumo neįvykdė Mokėjimų įstatymo 34 straipsnyje nustatytų mokėtojo pareigų ir neužtikrino, kad, be pareiškėjos, turinčios teisę naudotis mokėjimo priemone, personalizuotais saugumo duomenimis negalėtų pasinaudoti kiti asmenys.

Kaip ir minėta, pareiškėjos pateikti paaiškinimai apie mokėjimo operacijų įvykdymo aplinkybes iš esmės nesutampa su banko sistemų užfiksuotais duomenimis.

Ginčo byloje nustatyta, kad pareiškėja į savo mobilųjį telefoną 2021 m. spalio 3 d. 17 val. 42 min. gavo SMS žinutę, kurioje buvo pateikta aktyvi nuoroda su tekstu: *„SEB" programa uzblokuota del saugumo. Noredami to isvengti, spustelekite nuoroda: HK38721.com."* Pareiškėja teigė, kad šią SMS žinutę pamatė tik 2021 m. spalio 5 d., nes 2021 m. spalio 3 d. apskritai nesinaudojo savo mobiliuoju telefonu, todėl ir negalėjo paspausti SMS žinutėje pateiktos aktyvios nuorodos. Pareiškėja kategoriškai neigia spaudusi šią aktyvią nuorodą.

2021 m. spalio 3 d. 19 val. 22 min. ir 19 val. 24 min iš pareiškėjos sąskaitų banke buvo inicijuotos mokėjimo operacijos. Banko vidinių sistemų užfiksuotais duomenimis, mokėjimo operacijos inicijuotos iš IP adreso Nr. *duomenys neskelbiami* (Lietuvoje), kuris nepriklauso pareiškėjai, ir iš mobiliojo įrenginio *iPhone 8,4,* kuris taip pat nepriklauso pareiškėjai. Kauno apygardos prokuratūros Marijampolės apylinkės prokuratūros 2022 m. sausio 14 d. nutarime Sustabdyti ikiteisminį tyrimą Nr. *duomenys neskelbiami* (toliau – Nutarimas) nurodoma, kad ikiteisminio tyrimo metu buvo nustatytas asmuo – *duomenys neskelbiami*, kuriam priklauso IP adresas, iš kurio buvo inicijuotos mokėjimo operacijos. Tačiau ikiteisminio tyrimo metu apklausus minėtą asmenį, nebuvo nustatyta, kad jis neteisėtu būdu įgijo pareiškėjos mokėjimo priemonę ir kad būtent jis įvykdė mokėjimo operacijas. Nutarime nurodyta: „Lietuvos Respublikoje ikiteisminio tyrimo metu atlikti visi būtini proceso veiksmai, išnaudotos visos galimybės nustatyti nusikalstamą veiką padariusį asmenį, tačiau policijos pareigūnai asmenį, kuris neteisėtai prisijungė prie nukentėjusiosios banko sąskaitos, nenustatė." Šiame kontekste pažymėtina, kad pareiškėja Nutarimo neskundė, nors ir yra atstovaujama profesionalaus atstovo.

Pareiškėja tiek Lietuvos bankui, tiek ikiteisminio tyrimo pareigūnams teigė, kad 2021 m. spalio 3 d. nesijungė prie savo banko sąskaitos, apskritai jokių mokėjimo operacijų neinicijavo, o paskutinė jos pačios inicijuota 45,20 Eur mokėjimo operacija buvo 2021 m. spalio 2 d. už siuntinį DHL bendrovei. Pareiškėja tiek Lietuvos bankui, tiek ikiteisminio tyrimo metu paaiškino, kad ši 45,20 Eur mokėjimo operacija buvo įvykdyta sėkmingai – gavėjas gavo

pinigines lėšas. Papildomai Lietuvos bankui telefonu pareiškėja teigė, kad galbūt tretieji asmenys galėjo pasisavinti jos mokėjimo priemonę būtent tada, kai minėtą mokėjimo operacija buvo inicijuojama, tačiau pareiškėja teigė negalinti paaiškinti, kaip tai galėjo atsitikti, nes 45,20 Eur mokėjimo operaciją inicijavo ji pati, o gavėjas lėšas gavo.

Banko vidinių sistemų užfiksuotais duomenimis, 2021 m. spalio 3 d. 19 val. 15 min. 4 sek. buvo jungtasi prie pareiškėjos paskyros banke iš IP adreso Nr. *duomenys neskelbiami* (Lietuvoje), o 19 val. 15 min. 37 sek. naudojantis mobiliojo telefono įrenginiu *Samsung SM-A705FN* buvo sėkmingai įvykdyta autentifikacija – prisijungimas patvirtintas „Smart-ID" PIN1 bei PIN2 kodais. Pareiškėja Lietuvos bankui patvirtino, kad IP adresas Nr. *duomenys neskelbiami* ir mobiliojo telefono įrenginys *Samsung SM-A705FN* priklauso pareiškėjai. Įvertinus šiuos banko pateiktus vidaus sistemų duomenis, galima teigti, kad pareiškėjos teiginiai, kad 2021 m. spalio 3 d. ji nesinaudojo savo mobiliojo telefono įrenginiu ir nesijungė prie savo banko paskyros, yra neatitinkantys tikrovės. Kaip ir minėta, pareiškėja teigė, kad personalizuoti saugos duomenys buvo žinomi tik jai pačiai, vadinasi, niekas kitas be pačios pareiškėjos minėtų veiksmų atlikti negalėjo.

Banko sistemų duomenimis, po to, kai pareiškėja jungėsi prie savo banko paskyros, laikotarpiu nuo 19 val. 18 min. 41 sek. iki 19 val. 23 min. 54 sek. pareiškėjos „Smart-ID" PIN1 bei PIN2 kodai buvo įvesti trečiųjų asmenų įrenginyje *iPhone 8,4* ir pareiškėjos vardu sukurta nauja „Smart-ID" paskyra, kuria pasinaudojant buvo inicijuotos ir patvirtintos mokėjimo operacijos iš IP adreso Nr. *duomenys neskelbiami* Banko pateiktais duomenimis, bankas 19 val. 15 min. SMS žinute informavo pareiškėją apie pareiškėjos vardu sukurtą naują „Smart-ID" paskyrą. Kaip ir minėta, pareiškėja Lietuvos bankui teigė, kad 2021 m. spalio 3 d. savo mobiliuoju telefonu nesinaudojo, todėl šią banko žinutę pamatė tik 2021 m. spalio 5 d. Vis dėlto, banko vidinių sistemų duomenimis, yra užfiksuotas jungimasis prie pareiškėjos banko paskyros iš pareiškėjai priklausančio įrenginio ir IP adreso vos kelios sekundės po to, kai pareiškėja gavo banko SMS žinutę apie naujos „Smart-ID" paskyros sukūrimą (2021 m. spalio 3 d. 19 val. 15 min. 4 sek. buvo jungtasi prie pareiškėjos paskyros banke iš IP adreso Nr. *duomenys neskelbiami* (Lietuvoje), naudojantis mobiliojo telefono įrenginiu *Samsung SM-A705FN*). Taigi, remiantis banko vidinių sistemų duomenimis, galima teigti, kad pareiškėjos teiginys, kad ji banko SMS žinutę apie naujos „Smart-ID" paskyros sukūrimą pamatė tik 2021 m. spalio 5 d., neatitinka tikrovės. Pareiškėjai teigiant, kad jos mobiliojo telefono įrenginys visą laiką buvo tik jos žinioje, taip pat teigiant, kad niekam kitam ji nebuvo perdavusi ar kitaip atskleidusi savo personalizuotų prisijungimo prie banko sąskaitos duomenų, darytina išvada, kad niekas kitas negalėjo naudotis pareiškėjos mobiliuoju telefonu ir jos mokėjimo priemone, tik pati pareiškėja.

Ginčo byloje iš esmės nėra aiškios pareiškėjos mokėjimo priemonės praradimo aplinkybės, ypač atsižvelgiant į tai, kad pareiškėja kategoriškai neigia spaudusi aktyvią nuorodą, ir į tai, kad ikiteisminio tyrimo metu nustačius ir apklausus konkretų asmenį, kuriam priklauso IP adresas, iš kurio buvo inicijuotos mokėjimo operacijos, jo veiksmuose nebuvo nustatyta jokios neteisėtos veikos. Be to, kaip minėta, pačios pareiškėjos pateiktus paaiškinimus apie mokėjimo operacijų inicijavimo aplinkybes paneigia banko sistemų duomenys.

Teigdamas, kad pareiškėjos elgesys, dėl kurio ji prarado savo mokėjimo priemonę, turi didelio neatsargumo požymių, bankas remiasi argumentu, kad pareiškėja nesilaikė mokėtojui nustatytos pareigos saugoti personalizuotus saugos duomenis ir niekam jų neatskleisti. Banko teigimu, labiausiai tikėtina, kad pareiškėja paspaudė trečiųjų asmenų atsiųstą aktyvią nuorodą, joje suvedė savo personalizuotus saugos duomenis ir savo mobiliajame įrenginyje suvedė „Smart-ID" PIN1 ir PIN2 kodus. Taip pat pareiškėja, gavusi SMS žinutę iš banko, kad jos vardu yra sukurta nauja „Smart-ID" paskyra, nedelsdama nesikreipė į banką, nors pati naujos „Smart-ID" paskyros sukūrimo ir neinicijavo.

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 nurodytos neginčijamos neautorizuotos mokėjimo operacijos įvykdymo aplinkybės. Taigi, išvada dėl mokėtojo paprasto ar didelio neatsargumo, kaip vertinamojo pobūdžio aplinkybė, negali būti daroma izoliuotai, išsamiai neįvertinus viso neautorizuotos mokėjimo operacijos įvykdymo ir su juo susijusių aplinkybių konteksto.

Kriterijai, į kuriuos reikėtų atsižvelgti vertinant kaltės laipsnį, yra iš dalies suformuluoti Antrosios mokėjimo paslaugų direktyvos (toliau – PSD2) preambulės 72 punkte: „Siekiant įvertinti galimą mokėjimo paslaugų vartotojo aplaidumą ar didelį aplaidumą, reikėtų atsižvelgti į visas aplinkybes. Įtariamo aplaidumo įrodymai ir laipsnis paprastai turėtų būti vertinami pagal nacionalinę teisę. Tačiau nors aplaidumo sąvoka reiškia, kad pažeidžiamas įsipareigojimas elgtis rūpestingai, didelis aplaidumas turėtų reikšti daugiau nei vien aplaidumą ir apimti labai nerūpestingą elgesį; pavyzdžiui, tai būtų mokėjimo operacijos autorizavimui naudojamų saugumo požymių laikymas prie mokėjimo priemonės atviru ir trečiosioms šalims lengvai atskleidžiamu formatu."

Didelio neatsargumo sąvoka taip pat plėtojama Lietuvos Aukščiausiojo Teismo praktikoje. Kasacinis teismas yra išaiškinęs, kad „didelis neatsargumas kaip kaltės forma pasireiškia neprotingu arba išskirtiniu rūpestingumo nebuvimu, kai asmuo nėra tiek rūpestingas, kiek akivaizdžiai būtina esamomis aplinkybėmis" (Lietuvos Aukščiausiojo Teismo 2017 m. balandžio 13 d. nutartis civilinėje byloje Nr. e3K-3-180-378/2017, 29 punktas).

Kad būtų galima įvertinti, ar pareiškėja iki mokėjimo operacijos įvykdymo galėjo pastebėti, kad mokėjimo priemonė buvo neteisėtai pasisavinta, svarbūs ne tik banko pateikti sistemų išrašų duomenys apie mokėjimo operacijos įvykdymą, bet ir ginčo šalių paaiškinimai apie mokėjimo priemonės praradimo ir mokėjimo operacijos įvykdymo aplinkybes. Kaip ir buvo minėta, pareiškėjos pateikti paaiškinimai iš esmės prieštarauja banko vidinių sistemų užfiksuotiems duomenims ir neatitinka tikrovės. Nors bankas teigia, kad labiausiai tikėtina, kad pareiškėja tretiesiems asmenims savo personalizuotus saugos duomenis atskleidė besijungdama prie banko paskyros per SMS žinute gautą aktyvią nuorodą, tačiau iš ginčo byloje turimų pareiškėjos paaiškinimų ir ikiteisminio tyrimo metu nustatytų mokėjimo operacijų įvykdymo aplinkybių nėra galimybės daryti net ir tikėtinos prielaidos, kaip (teisėtai ar neteisėtai) tretieji asmenys galėjo įgyti pareiškėjos mokėjimo priemonę ir ja naudotis kaip sava. Ginčo byloje yra tik nustatytas faktas, kad mokėjimo operacijos buvo inicijuotos iš pareiškėjai nepriklausančio įrenginio ir IP adreso.

Ginčo byloje turimais duomenimis, tretiesiems asmenims pasinaudojus pareiškėjos personalizuotais saugos duomenimis ir savo mobiliajame telefone pareiškėjos vardu sukūrus naują „Smart-ID" paskyrą, bankas pareiškėjai į jos mobilųjį telefoną atsiuntė SMS žinutę, kad pareiškėjos vardu buvo sukurta nauja „Smart-ID" paskyra, ir, jeigu pati naujos paskyros sukūrimo neinicijavo, pareiškėja nedelsdama turi kreiptis į banką telefonu (*„Gerb. Kliente, Jūsų vardu SEB banke registruojama „Smart-ID Basic" paskyra. Jei to neinicijavote, prašom kuo skubiau susisiekti tel. +370 5 268 2800. SEB bankas*"). Banko pateiktais duomenimis, pareiškėja šią banko jai siųstą SMS žinutę gavo 2021 m. spalio 3 d. 19 val. 15 min., tačiau nedelsdama nesikreipė į banką. Pareiškėja į banką kreipėsi tik 2021 m. spalio 5 d., nors, ginčo byloje nustatytais duomenimis, pati pareiškėja 2021 m. spalio 3 d. 19 val. 15 min. 4 sek. jungėsi prie savo banko sąskaitos naudodamasi savo mobiliajame telefone įdiegta „Smart-ID" paskyra. Taigi, nors pareiškėja teigia nemačiusi šios banko žinutės, nes tą dieną apskritai nesinaudojo savo mobiliuoju telefonu, tačiau turimi įrodymai patvirtina, kad vis dėlto pareiškėja naudojosi savo mobiliuoju telefonu ir jungėsi prie savo banko paskyros (pareiškėja teigė, kad mobilusis telefonas buvo jos žinioje ir personalizuoti saugos duomenys buvo žinomi tik jai pačiai). Vadinasi, pareiškėja banko siųstą SMS žinutę apie naujos „Smart-ID" paskyros sukūrimą turėjo ir galėjo pamatyti ir, jeigu ji pati neinicijavo naujos „Smart-ID" paskyros sukūrimo kitame įrenginyje, turėjo nedelsdama kreiptis į banką. Tačiau pareiškėja į banką kreipėsi tik po dviejų dienų – 2021 m. spalio 5 d. Galima daryti išvadą, kad pareiškėja, pastebėjusi galimą savo mokėjimo priemonės praradimą, elgėsi labai nerūpestingai ir delsė kreiptis į banką, taip prarado galimybę užkirsti kelią neautorizuotų mokėjimo operacijų iš jos banko sąskaitos vykdymui.

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). Taisyklių 1 priedo 10 skyriuje nurodoma, kad banko suteiktą mokėjimo priemonę ir su ja susijusius personalizuotus saugumo duomenis mokėtojas privalo saugoti ir imtis visų reikiamų veiksmų, kad personalizuoti saugumo duomenys nebūtų atskleisti jokiems kitiems asmenims. Taigi, įvertinus ginčo byloje turimus

duomenis bei ginčo šalių paaiškinimus apie mokėjimo operacijų įvykdymo aplinkybes, galima teigti, kad pareiškėjos personalizuoti saugos duomenys buvo žinomi ne tik pareiškėjai, bet ir tretiesiems asmenims, kurie buvo įgiję (teisėtu ar neteisėtu) būdu galimybę naudotis pareiškėjos mokėjimo priemone kaip sava, o pareiškėja, sužinojusi apie neautorizuotą mokėjimo priemonės naudojimą (gavusi SMS žinutę apie naujos „Smart-ID" paskyros sukūrimą), nesikreipė į banką ir nepranešė apie veiksmus, susijusius su jos mokėjimo priemone, kurių ji pati neinicijavo. Galima teigti, kad pareiškėja neįvykdė Mokėjimų įstatymo 34 straipsnyje reglamentuojamų mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigų.

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 kaip 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 pareiškėja iš esmės kategoriškai neigia, kad tretiesiems asmenims atskleidė savo prisijungimo prie paskyros duomenis bei „Smart-ID" PIN1 ir PIN2 kodus, kuriais buvo patvirtintas naujos „Smart-ID" paskyros sukūrimas, tačiau iš esmės jos pateikti paaiškinimai yra klaidingi – neatitinkantys objektyvių banko vidaus sistemose užfiksuotų duomenų, tai kelia abejonių ir dėl pačios pareiškėjos sąžiningumo. Ginčo byloje yra akivaizdu, kad galimybę naudotis pareiškėjos mokėjimo priemone kaip sava turėjo ne tik pati pareiškėja, bet ir tretieji asmenys, tačiau, pareiškėjai kategoriškai neigiant, kad ji spaudė SMS žinute atsiųstą aktyvią nuorodą, ir teigiant, kad personalizuoti saugos duomenys buvo žinomi tik jai vienai, iš esmės nėra galimybės nustatyti, kaip (teisėtai ar neteisėtai) tretieji asmenys įgijo galimybę naudotis pareiškėjos mokėjimo priemone. Pareiškėjos bendradarbiavimo trūkumas iš esmės ir lemia tai, kad neturima duomenų, iš kurių pareiškėjos elgesį prarandant mokėjimo priemonę būtų galima vertinti tik kaip neatsargų ir todėl visi dėl mokėjimo operacijos patirti nuostoliai turėtų tekti bankui.

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, bankas neprivalo pareiškėjai grąžinti neautorizuotų mokėjimo operacijų lėšų ir todėl pareiškėjos 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 pareiškėjos X.X. reikalavimą.

Lietuvos banko sprendimas dėl ginčo esmės yra rekomendacinio pobūdžio ir teismui neskundžiamas. Vartotojui ir finansų rinkos dalyviui išlieka teisė dėl tapataus ginčo dalyko kreiptis į teismą arba kitą ginčų nagrinėjimo instituciją įstatymų nustatyta tvarka. Kreipimasis į teismą po Lietuvos banko sprendimo dėl ginčo esmės priėmimo nelaikomas šio Lietuvos banko sprendimo apskundimu. Ginčo šalys turi pareigą pranešti Lietuvos bankui, jeigu viena iš ginčo šalių pareiškia ieškinį bendrosios kompetencijos teismui, prašydama nagrinėti tapatų ginčą iš esmės.

Direktorius Arūnas Raišutis