LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

SPRENDIMAS DĖL X. X. IR *REVOLUT BANK UAB* GINČO NAGRINĖJIMO

2023 m. balandžio 20 d. Nr. 429-220
Vilnius

Lietuvos bankas gavo X. X. (toliau – pareiškėja) kreipimąsi, kuriuo prašoma išnagrinėti tarp pareiškėjos ir *Revolut Bank UAB* (toliau – bankas) kilusį ginčą.

N u s t a t y t a:

2022 m. gruodžio 6 d. pareiškėja kreipėsi į banką per banko mobiliąją programėlę ir nurodė, kad neatpažįsta mokėjimų kortele. Automatiniam atsakikliui identifikavus raktinius žodžius, pareiškėjai buvo pateiktas standartizuotas atsakymas, kokių veiksmų reikia imtis, jeigu pareiškėja turi pagrindą manyti, kad jos mokėjimo priemonių duomenis galėjo neteisėtai sužinoti ir (ar) jais pasinaudoti tretieji asmenys.

2022 m. gruodžio 8 d. pareiškėja kreipėsi į banką pakartotinai ir nurodė, kad 2022 m. gruodžio 6 d. tapo sukčiavimo auka, nes buvo neteisėtai panaudota jai banko išduota mokėjimo kortelė. Pareiškėja pasiteiravo dėl galimybės susigrąžinti mokėjimų lėšas, nes buvo trečiųjų asmenų informuota, kad prarastos lėšos dėl ginčijamų mokėjimo operacijų jai bus grąžintos. Bankui paprašius detalizuoti įvykio aplinkybes, pareiškėja nurodė, kad su ja susisiekė asmuo, prisistatęs banko darbuotoju, ir pranešė apie galimai vykdomą sukčiavimą pareiškėjos atžvilgiu. Papildomai pareiškėja nurodė, kad tariamas banko atstovas pateikė didelės vertės pačios pareiškėjos autorizuotos mokėjimo operacijos, kuri, pasak pareiškėjai skambinusio asmens, galimai buvo neteisėta, detales ir prašė pareiškėjos patvirtinti tapatybę, padiktuojant saugos kodą, kuris jai buvo išsiųstas trumpąja SMS žinute. Pareiškėja nurodė, kad duomenų, susijusių su asmenine mokėjimo sąskaita ar jos saugumo duomenimis, jokiems tretiesiems asmenims neatskleidė, tačiau asmeniui, prisistačiusiam banko darbuotoju, pasakė patvirtinimo saugos kodą, gautą SMS žinute.

Atsižvelgdamas į pareiškėjos nurodytas aplinkybes, bankas pradėjo vidinį tyrimą dėl 2022 m. gruodžio 6 d. įvykdytų pareiškėjos ginčijamų 7 mokėjimo operacijų, kurių bendra vertė 2 148 GBP (2 425,63 Eur) (toliau – Ginčijami mokėjimai).

Banko patarta pareiškėja laikotarpiu nuo 2022 m. gruodžio 8 d. iki 2022 m. gruodžio 10 d. pateikė 7 prašymus inicijuoti lėšų grąžinimo procedūrą (angl. *chargeback*) Ginčijamų mokėjimų atžvilgiu.

2022 m. gruodžio 10 d. bankas priėmė sprendimą netenkinti pareiškėjos prašymų inicijuoti lėšų grąžinimo procedūrą, nes pareiškėjos Ginčijamų mokėjimų vykdymo aplinkybės nepriskirtinos prie tarptautinės mokėjimo kortelių organizacijos „MasterCard" taisyklėse nustatytų atvejų, kada tokia procedūra yra galima.

Pareiškėja nesutinka su tokiu banko sprendimu ir atsisakymu kitaip kompensuoti pareiškėjos dėl įvykdytų Ginčijamų mokėjimų atsiradusius nuostolius.

Pareiškėjos teigimu, bankas nesuteikia savo klientams, taigi, ir pareiškėjai, bei jų mokėjimo sąskaitose esančioms lėšoms tokios pat apsaugos kaip kiti komerciniai bankai. Bankas, pareiškėjos manymu, taip pat netaiko tokių pat apsaugos nuo apgaulingų mokėjimo operacijų priemonių kaip kiti komerciniai bankai, tinkamai nevykdo mokėjimo operacijų stebėsenos, tai, pareiškėjos vertinimu, šiuo atveju ir lėmė, kad Ginčijami mokėjimai buvo įvykdyti sukčiams. Kreipimesi pareiškėja prašo rekomenduoti bankui atlyginti pareiškėjos nuostolius dėl įvykdytų Ginčijamų mokėjimų.

Bankas nesutinka tenkinti pareiškėjos reikalavimo. Bankas mano, kad Ginčijami mokėjimai buvo pareiškėjos tinkamai autorizuoti, todėl bankas negali būti įpareigotas grąžinti

pareiškėjai šių mokėjimų sumos. Bankui, jo vertinimu, veikus pagal teisės aktų bei paslaugų teikimo sąlygų nuostatas ir tinkamai įvykdžius gautus mokėjimo nurodymus, t. y. nesant banko neteisėtų veiksmų, negali būti keliamas ir banko civilinės atsakomybės klausimas, nes netenkinama būtinoji civilinės atsakomybės taikymo sąlyga. Bankas papildomai pažymi, kad pareiškėja, nepaisydama SMS pranešime nurodytos informacijos dėl vienkartinio saugos kodo paskirties ir atidžiai neįvertinusi tariamo banko darbuotojo reikalavimo pateikti saugos kodą tapatybei patvirtinti, taigi, aplaidžiai ir nerūpestingai, pati savo aktyviais veiksmais trečiajam asmeniui suteikė galimybę pridėti jos mokėjimo priemonę prie *Apple Pay* įrenginio.

Atsižvelgdamas į išdėstytą informaciją ir argumentus, bankas prašė atmesti pareiškėjos reikalavimą.

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 42^1 straipsnyje reglamentuojamų patikrinimų, skirtų faktinėms aplinkybėms dėl Lietuvos banko priežiūrimo finansų rinkos dalyvio galimai padaryto Lietuvos banko kompetencijai priskirtų teisės aktų reikalavimų pažeidimo nustatyti ir įvertinti. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą ir jo pagrindu priima sprendimą.

Ginčas kilo dėl to, kad bankas atsisakė grąžinti pareiškėjai jos mokėjimo kortele, naudojant *Apple Pay* mokėjimo nurodymo patvirtinimo metodą, atliktų Ginčijamų mokėjimų, kurių bendra vertė 2 148 GBP, sumą.

Pareiškėja teigia nedavusi sutikimo atlikti Ginčijamus mokėjimus, neigia juos autorizavusi ir (ar) pridėjusi savo mokėjimo kortelę prie *Apple Pay* sistemos iš naujo įrenginio. Pareiškėja teigia banko darbuotojais prisistačiusiems asmenims atskleidusi tik SMS žinute gautą vienkartinį saugos kodą, to pakako, kad tretieji asmenys jos mokėjimo kortelę pridėtų prie *Apple Pay* sistemos. Pareiškėjos manymu, bankas neužtikrino jos mokėjimo kortelės sąskaitoje esančių lėšų saugumo, neįsidiegė pakankamai apsaugos priemonių tam, kad nesąžiningi, neautorizuoti mokėjimai neįvyktų ir tai lėmė, kad Ginčijami mokėjimai buvo įvykdyti, o jų lėšos iš pareiškėjos mokėjimo kortelės sąskaitos buvo nurašytos. Bankas teigia, kad Ginčijami mokėjimai buvo įvykdyti naudojant *Apple Pay* mokėjimo nurodymo patvirtinimo metodą. Tam, kad pareiškėjos mokėjimo kortelė būtų pridėta prie *Apple Pay* sistemos, turėjo būti panaudoti pareiškėjos mokėjimo kortelės duomenys, o pridėjimas patvirtintas banko į sutartyje nurodytą telefono numerį išsiųstoje žinutėje pateiktu vienkartiniu saugos kodu. Banko vertinimu, Ginčijamus mokėjimus autorizavo pati pareiškėja arba pareiškėja dėl didelio neatsargumo atskleidė tretiesiems asmenims savo mokėjimo kortelės duomenis ir vienkartinį saugos kodą, dėl to tretieji asmenys galėjo įgyti galimybę inicijuoti Ginčijamus mokėjimus *Apple Pay* mokėjimo metodu.

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

Siekiant išspręsti šį pareiškėjos ir banko ginčą, Lietuvos banko vertinimu, būtina nustatyti, ar: *1) Ginčijami mokėjimai laikytini autorizuotais; 2) bankas privalo grąžinti pareiškėjai Ginčijamų mokėjimų sumą; 3) pagrįstai pareiškėja teigia, kad banko paslaugos buvo teikiamos nesaugiai ir tai galėjo lemti pareiškėjos nuostolius*.

1. Dėl Ginčijamų mokėjimų 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).

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

Banko ir pareiškėjos bendrąją sutartį sudarančių banko privatiems klientams taikomų sąlygų 14 punkte nurodyta, kad mokėjimai gali būti autorizuojami įvedant mokėjimo kortelės duomenis (kortelės numerį, galiojimo datą, CVV kodą) arba PIN kodą. Sutikimas taip pat gali būti duotas paliečiant kortele terminalą (bekontaktis atsiskaitymas) ar atliekant kitus veiksmus su elektroniniu kortelių skaitytuvu. Šiuos veiksmus bankas laiko mokėtojo sutikimu atlikti mokėjimus iš banko sąskaitos[1]. Atsižvelgiant į tai, kad bendroji sutartis (ją sudarančios banko privatiems klientams taikomos sąlygos) nustato banko ir pareiškėjos tarpusavio santykius, ir įvertinus tai, kad mokėjimo kortelės duomenys ir PIN kodo slaptažodis yra personalizuoti saugumo duomenys, kurie pripažįstami neskelbtinais mokėjimo duomenimis (Mokėjimų įstatymo 2 straipsnio 41 dalis), darytina išvada, kad bendrojoje sutartyje nurodyti mokėjimo operacijos autorizavimo būdai (suvedant mokėjimo kortelės duomenis ir (arba) PIN kodą) pareiškėjos ir banko santykiuose laikytini pareiškėjos sutikimu įvykdyti mokėjimo operaciją tik tada, kai pati pareiškėja pateikia mokėjimo kortelės duomenis ir (arba) suveda PIN kodo slaptažodį, norėdama įvykdyti mokėjimo operaciją.

Banko kartu su atsiliepimu pateiktais vidaus sistemos duomenimis, visi pareiškėjos Ginčijami mokėjimai atlikti tuo pačiu mobiliuoju įrenginiu (įrenginio pavadinimas matomas banko sistemose –„Kishi's iPhone"), kuris kaip *Apple Pay* mokėjimo įrenginys prie *Apple Pay* sistemos buvo pridėtas ir autorizuotas, kaip nurodė bankas, pačios pareiškėjos prieš inicijuojant Ginčijamus mokėjimus būtent jų įvykdymo dieną, t. y. 2022 m. gruodžio 6 d.

Pareiškėja neigia ne tik autorizavusi Ginčijamus mokėjimus, bet ir prieš įvykdant Ginčijamus mokėjimus atskleidusi tretiesiems asmenims savo mokėjimo kortelės duomenis ir (ar) juos kur nors suvedusi. Pareiškėja pripažįsta atskleidusi tik SMS žinute gautą vienkartinį saugos kodą, to, pareiškėjos teigimu, užteko, kad jos mokėjimo kortelė būtų susieta su *Apple Pay* mokėjimo metodu.

Vis dėlto, kaip paaiškino bankas atsiliepime, norėdamas pridėti mokėjimo kortelę prie *Apple Pay*, asmuo turi atlikti aktyvius veiksmus, numatytus *Apple Pay* sąlygose[2]: 1) įrenginyje, kuriuo siekiama atlikti *Apple Pay* mokėjimą, reikia įvesti mokėjimo kortelės duomenis (kortelės numerį, saugos kodą CVV, kita) arba nuskaityti mokėjimo kortelę; 2) suvedęs mokėjimo kortelės duomenis, asmuo turi perskaityti mokėjimo sąlygas ir su jomis sutikti; 3) siekdamas patvirtinti mokėjimo kortelės duomenų teisingumą, bankas patikrina pateiktą informaciją. Nustačius, kad pateikta mokėjimo kortelė yra aktyvi ir duomenys teisingi, asmuo turi atlikti banko, kuris išdavė mokėjimo kortelę, nurodymus. Šiuo atveju įvesti vienkartinį saugos kodą (kuris galioja 30 min. po kodo išsiuntimo), kuris yra išsiunčiamas į telefono numerį, susietą su mokėjimo kortelės savininko banko sąskaita. Banko pateiktais duomenis, pareiškėjai jos bankui nurodytu telefonu numeriu buvo išsiųsta SMS žinutė su vienkartiniu saugos kodu, tai, banko teigimu, reiškia, kad pirmiau nurodyti veiksmai, skirti pareiškėjos mokėjimo kortelei prie *Apple Pay* įrenginio pridėti, – pareiškėjos mokėjimo kortelės duomenų (numeris, CVV kodas) suvedimas, taip pat buvo atlikti.

Atsiliepime, net ir atsižvelgdamas į tai, kad Ginčijami mokėjimai buvo inicijuoti jų įvykdymo dieną, prie *Apple* Pay sistemos pridėjus pareiškėjos mokėjimo kortelę naujame įrenginyje, kuris, kaip teigia bankas, nepriklauso pareiškėjai, bankas teigė, kad šie mokėjimai laikytini autorizuotais, nes mokėjimo kortelė inicijuojant Ginčijamus mokėjimus buvo pareiškėjos žinioje, o prie *Apple Pay* sistemos pridėta suvedus į pareiškėjos mobilųjį telefoną SMS žinute atsiųstą vienkartinį saugos kodą.

Vis dėlto, įvertinus pareiškėjos paaiškinimus apie Ginčijamų mokėjimų atlikimo aplinkybes ir iš banko vidaus sistemų surinktus duomenis, negalima daryti išvados, kad šie mokėjimai buvo inicijuoti ir patvirtinti pačios pareiškėjos, t. y. su jos žinia ir sutikimu.

---

[1] Tekstas anglų k.: „*You can also make payments or withdraw cash using your Revolut Card. You can do this by entering the details of your Revolut Card (the card number, expiry date and CVC number) or your PIN. We will consider these actions as you giving consent to make payments or withdraw cash from your Revolut account. You also give your consent to make payments from your Revolut Card by: touching your Revolut Card at the terminal (a 'contactless' transaction) and taking other actions on the electronic card reader <…>*"

[2] https://support.apple.com/lt-lt/HT204506

Nors, ginčo bylos duomenimis, pareiškėjos mokėjimo kortelė prie *Apple Pay* sistemos naujame įrenginyje galėjo būti pridėta suvedant ne tik šios kortelės duomenis (kortelės numerį, CVC kodą), bet ir banko į pareiškėjos mobilųjį telefoną SMS žinute atsiųstą vienkartinį saugos kodą, nustatyti ir banko neginčijami duomenys leidžia pagrįstai abejoti, ar mokėjimo priemonė, kuria atlikti Ginčijami mokėjimai, buvo tik pareiškėjos žinioje. Dėl to, pačiai pareiškėjai neigiant Ginčijamų mokėjimų autorizavimo aplinkybę ir esant pagrįstų duomenų apie įvykusį sukčiavimo atvejį – taigi, kad pareiškėjos mokėjimo priemone ir jos personalizuotais saugumo duomenimis, be pareiškėjos žinios ir nesant jos valios, galėjo neteisėtai pasinaudoti tretieji asmenys, negalima daryti išvados, kad pareiškėjos mokėjimo kortele atlikti Ginčijami mokėjimai buvo jos autorizuoti, t. y. inicijuoti ir patvirtinti eesant pačios pareiškėjos sutikimui, kaip tai suprantama Mokėjimų įstatymo 29 straipsnio 1 dalies kontekste. Atsižvelgdamas į tai Lietuvos bankas daro išvadą, kad Ginčijami mokėjimai laikytini neautorizuotais.

2. *Dėl neautorizuotų mokėjimo operacijų pasekmių ir pareiškėjos teisės į Ginčijamų mokėjimų sumos grąžinimą*

Pagal Mokėjimų įstatymo 38 straipsnio 1 dalį, joje nurodytomis sąlygomis ir tvarka mokėtojo mokėjimo paslaugų teikėjas privalo grąžinti mokėtojui neautorizuotos mokėjimo operacijos sumą. Mokėjimų įstatymo 39 straipsnis nustato šios taisyklės taikymo išimtis.

Vadovaujantis Mokėjimų įstatymo 39 straipsnio 3 dalimi, 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[3] nustatytų pareigų.

Mokėjimų įstatymas, kaip minėta, aiškiai nustato, kad tuo atveju, 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 (Mokėjimų įstatymo 37 straipsnio 3 dalis).

Įvertinus nurodytas Mokėjimų įstatymo nuostatas, galima teigti, kad mokėtojo mokėjimo paslaugų teikėjas gali būti visiškai atleistas nuo pareigos grąžinti mokėtojui neautorizuotos mokėjimo operacijos sumą tik tuo atveju, jeigu pateikia mokėtojo sukčiavimo (nesąžiningumo arba tyčios) arba didelio neatsargumo įrodymų, t. y. jei pagal mokėjimo paslaugų teikėjo pateiktus įrodymus nustatoma, kad mokėtojas ne tik neįvykdo vienos ar kelių jam Mokėjimų įstatyme nustatytų pareigų, bet ir padaro tai elgdamasis nesąžiningai arba tyčia ar būdamas labai neatsargus (Mokėjimų įstatymo 37 straipsnio 3 dalis ir 39 straipsnio 3 dalis).

Aplinkybių ir duomenų, kaip ir šalių ginčo dėl to, kad pareiškėja galėjo veikti nesąžiningai arba tyčia, įskaitant sukčiavimą, nėra. Bankas sprendimą nekompensuoti pareiškėjos nuostolių grindžia vertinimu, kad Ginčijami mokėjimai buvo autorizuoti tinkamai. Be to, bankas mano, kad pareiškėjos elgesiui būdingas ir didelis neatsargumas.

Tai reiškia, kad, atsižvelgiant į pirmiau minėtas Mokėjimų įstatymo nuostatas, siekiant įvertinti, ar bankas pagrįstai atsisako kompensuoti pareiškėjos nuostolius, susijusius su Ginčijamų mokėjimų įvykdymu, ir ar pareiškėjai galėtų būti taikoma Mokėjimų įstatymo 39 straipsnio 3 dalis, būtina nustatyti, ar pareiškėjos elgesys atskleidžiant tam tikrus personalizuotus mokėjimo priemonės (mokėjimo kortelės) požymius ir (ar) kiti veiksmai, dėl kurių galėjo būti įvykdyti Ginčijami mokėjimai, vertintini kaip didelis neatsargumas, dėl kurio visi jos reikalaujami atlyginti nuostoliai turėtų tekti pačiai pareiškėjai.

Pirmiau minėtame Mokėjimų įstatymo 34 straipsnyje nustatyta viena iš mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigų – naudotis mokėjimo priemone pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas.

[3] 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 (Mokėjimų įstatymo 34 straipsnio 2 dalis).

Panašias pareigas nustato banko ir pareiškėjos bendrąją sutartį sudarančių banko privatiems klientams taikomų sąlygų 9 dalis, kurioje nustatyta, kad: „darome viską, ką galime, kad apsaugotume jūsų pinigus. To paties prašome ir jūsų saugoti savo saugumo informaciją ir „Revolut" kortelę. Tai reiškia, jog neturėtumėte savo saugumo informacijos laikyti šalia „Revolut" kortelės ir turėtumėte juos paslėpti arba apsaugoti, jei kur nors užsirašote ar laikote. Savo saugumo informacijos nepateikite niekam kitam, išskyrus atvirosios bankininkystės paslaugų teikėją ar trečiosios šalies teikėją, besilaikantį teisės aktų reikalavimų<...>"

Taigi, aptartos privatiems klientams taikomų sąlygų nuostatos aiškiai nustato, kad už tapatybės priemonės personalizuotų saugumo duomenų konfidencialumą yra atsakingas mokėtojas, šiuo atveju – pareiškėja. Atsižvelgiant į tai, manytina, kad pareiškėjos elgesys būtų laikomas atitinkančiu mokėjimo priemonės išdavimą ir naudojimą reglamentuojančio susitarimo sąlygas, jei būtų nustatyta, kad ji ėmėsi adekvačių veiksmų (arba nuo tam tikrų veiksmų susilaikė), kad būtų tinkamai užtikrintas banko išduotų mokėjimo priemonių personalizuotų saugumo duomenų, sudarančių sąlygas inicijuoti ir tvirtinti mokėjimus, konfidencialumas.

Vadovaujantis ginčo byloje esančiais banko vidaus sistemų duomenimis, pareiškėjos Ginčijami mokėjimai buvo įvykdyti mokėjimo kortele, panaudojant *Apple Pay* mokėjimo metodą. Banko teigimu, kad būtų galima atsiskaityti naudojant *Apple Pay* mokėjimo metodą, būtina mokėjimo kortelę pridėti prie *Apple Pay* sistemos. Mokėjimo kortelei prie *Apple Pay* sistemos pridėti taikoma saugesnio autentiškumo patvirtinimo procedūra, kurios metu reikia ne tik pateikti mokėjimo kortelės duomenis, bet ir suvesti vienkartinį saugos kodą[4], kuris, pagal banko pateiktus įrodymus, šiuo atveju ir buvo suvestas. Bankas nurodė, kad jokių techninių trikdžių atliekant Ginčijamus mokėjimus nebuvo neužfiksuota, taip pat nebuvo užfiksuota jokių trečiųjų asmenų įsilaužimo į pareiškėjos mokėjimo kortelės sąskaitą banko programėlėje požymių.

Įrodymų pakankamumas civiliniame procese grindžiamas tikėtinumo taisykle (tikimybių pusiausvyros principas). 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 nebuvus[5].

Tad nors pareiškėja teigė, kad jokių savo mokėjimo priemonių personalizuotų saugumo duomenų ir (ar) kokių nors kitų savo duomenų niekam nėra atskleidusi, o mokėjimo kortelės ir (ar) jos valdymo kontrolės niekada nebuvo praradusi, ginčo byloje nustatyta, kad pareiškėjos mokėjimo kortelė prie *Apple Pay* sistemos naujame įrenginyje galėjo būti pridėta tik suvedus mokėjimo kortelės numerį ir šios kortelės CVC kodą, taip pat, ginčo byloje esančiais įrodymais ir šalių neginčijamomis aplinkybėmis, būtent į pareiškėjos mobilųjį telefoną atsiųstą vienkartinį saugos kodą. Nesant kitų galimybių nustatyti ir (ar) nenustačius kitokias aplinkybes pagrindžiančių duomenų, kaip pareiškėjos mokėjimo priemonių personalizuoti saugumo duomenys be pačios pareiškėjos veiksmų galėjo tapti žinomi tretiesiems asmenims, kai, pareiškėjos teigimu, jos mobilusis telefonas ir (ar) mokėjimo kortelė buvo jos žinioje, neginčijant konstatuotos aplinkybės, kad Ginčijami mokėjimai yra neautorizuoti ir jų įvykdyti savo valia pareiškėja nesiekė, labiau tikėtina, kad būtent pati pareiškėja, galbūt nesuprasdama atliekamų veiksmų reikšmės ir pasekmių, atskleidė tretiesiems asmenims visus duomenis, būtinus jos mokėjimo kortelei pridėti prie *Apple Pay* sistemos naujame įrenginyje, kuriuo vėliau ir buvo patvirtinti visi Ginčijami mokėjimai.

Taisyklių 45 punktas nustato, kad vartojimo ginčai Lietuvos banke nagrinėjami laikantis rungimosi principo – 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. Be to, pagal Taisyklių 43 punktą, Lietuvos bankas ginčą nagrinėja vertindamas ginčo šalių pateiktus rašytinius ir (ar) daiktinius įrodymus.

Tad nors pareiškėja neigia bet kokių su jos banko mokėjimo kortele susijusių duomenų atskleidimą tretiesiems asmenims, tarp jų ir suvedimą galimai nelegaliose interneto svetainėse prieš įvykdant Ginčijamus mokėjimus, vis dėlto nustatytos aplinkybės leidžia konstatuoti

---

[4] Pagal pirmiau minėtas *Apple Pay* sąlygas, vienkartinis saugos kodas SMS žinute banko kliento telefono numeriu yra siunčiamas tik tuomet, kai suvedami teisingi mokėjimo kortelės, kurią siekiama pridėti prie *Apple Pay* įrenginio, duomenys.

[5] 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.

priešingai.

Pareiškėja, pateikdama paaiškinimus dėl Ginčijamų mokėjimų įvykdymo aplinkybių ir kartu dėl bankui keliamo reikalavimo pagrįstumo, nurodė, kad Ginčijamų mokėjimų įvykdymo dieną su ja susiekė asmuo, prisistatęs banko darbuotoju[6], ir nurodė, kad bankas pastebėjo įtartiną veiklą pareiškėjos mokėjimo sąskaitoje. Pareiškėjos teigimu, skambinęs asmuo žinojo jos tą dieną įvykdytos didelės apimties mokėjimo operacijos detales, kurias, kaip ir faktą, kad šią operaciją inicijavo ir autorizavo pati, pareiškėja patvirtino. Skambinęs asmuo pareiškėjai nurodė, kad ji turės šią informaciją patvirtinti pasakydama skambinusiam asmeniui saugos kodą, kurį netrukus gaus SMS žinute. Kaip pažymi pareiškėja, gautas ir telefonu padiktuotas vienkartinis kodas leido skambinusiam asmeniui, kuris buvo sukčius, susieti pareiškėjos banko išduotą mokėjimo kortelę su *Apple Pay* mokėjimo metodu ir įvykdyti pirmąjį iš Ginčijamų mokėjimų. Pamačiusi, kad buvo įvykdytas pirmasis Ginčijamas mokėjimas, pareiškėja nusprendė imtis veiksmų, tačiau iš banko mobiliojoje programėlėje nurodytos informacijos sužinojo, kad tokiais atvejais mokėjimo kortelė, kuria galimai atlikta ginčytina mokėjimo operacija, yra nedelsiant užblokuojama, todėl siūloma prieš atliekant šį veiksmą įsitikinti, ar ginčijama mokėjimo operacija iš tiesų yra neautorizuota paties mokėtojo. Atsižvelgdama į tai, pareiškėja, jos teigimu, nusprendė kuriam laikui atsisakyti mokėjimo kortelės blokavimo ir patikrinti savo mokėjimo kortelės sąskaitos išrašą. Pareiškėja teigia, kad tuo metu, kai tikrino mokėjimo kortelės sąskaitos išrašą, pastebėjo, kad įvykdytas antrasis Ginčijamą mokėjimas, todėl iškart užblokavo savo mokėjimo kortelę.

Kreipimesi nurodytomis aplinkybėmis, po kelių minučių pareiškėjai vėl paskambino asmuo, prisistatęs banko darbuotoju, ir nurodė, kad jos mokėjimo kortelės sąskaitoje buvo pastebėta įtartina veikla. Pareiškėja patvirtino, kad jos mokėjimo sąskaita neteisėtai naudojosi trečiasis asmuo, ir paklausė skambinusio asmens, ką turėtų daryti tokioje situacijoje. Pareiškėja teigia buvusi informuota, kad nesijaudintų, nes bankas tokiais atvejais kompensuoja klientams dėl sukčiavimo prarastas lėšas. Pareiškėja skambinusio asmens taip pat buvo informuota, kad jis „mato dar daugiau mokėjimo operacijų pareiškėjos mokėjimo sąskaitoje ir jos dar nėra įvykdytos", tačiau jų skambinantis asmuo, tariamas banko darbuotojas, negali atšaukti, nes pareiškėjos mokėjimo kortelė yra užblokuota. Pareiškėja, kaip pripažįsta pati, tuomet atblokavo savo mokėjimo kortelę, o po šio veiksmo buvo įvykdyti likusieji 5 Ginčijami mokėjimai.

Pareiškėja kreipimesi pažymi, kad pirmąkart jai skambinusio asmens, prisistačiusio banko darbuotoju (t. y. sukčiaus), telefono numerį jos telefonas identifikavo kaip banko telefono numerį, todėl šio asmens nurodymai, kaip ir aplinkybė, kad jis žinojo pareiškėjos neseniai įvykdytos mokėjimo operacijos detales, nesuteikė pagrindo pareiškėjai suabejoti šio asmens patikimumu[7].

Vis dėlto būtina pabrėžti, kad duomenų, kurie patvirtintų pareiškėjos teiginius, kad jai pirmąkart skambinęs asmuo – tariamas banko darbuotojas, telefoninio pokalbio metu iš tiesų būtų nurodęs konfidencialias, tik pareiškėjai žinotinas jos autorizuotos didelės vertės mokėjimo operacijos detales, ginčo byloje nėra. Kita vertus, sprendžiant dėl pareiškėjos elgesio ir galimo neatsargumo laipsnio, turi būti atsižvelgti į tai, kad nors pareiškėja po pirmų dviejų Ginčijamų mokėjimų įvykdymo suprato buvusi apgauta sukčių ir užblokavo savo mokėjimo kortelę, tačiau tuomet, kai iškart sulaukė kito jai nepažįstamo asmens, vėl prisistačiusio banko darbuotoju ir nurodžiusio, kad skambina tuo pačiu tikslu – perspėti dėl galimai įtartinų, nesąžiningų mokėjimo operacijų iš pareiškėjos mokėjimo sąskaitos, skambučio, ir šįkart nesuabejojo skambinusio asmens pateiktos informacijos ir jo nurodymo atblokuoti mokėjimo kortelę patikimu. Taigi, pareiškėja pakartotinai jai paskambinusio nepažįstamo asmens nurodytos informacijos bei pateiktų nurodymų pagrįstumo papildomai nepatikrino ir mokėjimo kortelę nedelsdama ir nesudvejojusi atblokavo, taip sudarydama sąlygas tretiesiems asmenims įvykdyti likusius 5 Ginčijamus mokėjimus.

Išanalizavęs ginčo byloje esančius duomenis ir kitas nustatytas aplinkybes, net ir įvertinęs tai, kad trečiųjų asmenų (sukčių) veiksmai, apsimetant banko darbuotojais, iš tiesų galėjo sukurti klaidinantį pirminį įspūdį, Lietuvos bankas mano, kad pareiškėjos elgesys negali būti vertinamas kaip atsargus ir apdairus ar tik neatsargus.

Kaip nustatyta, pridedant pareiškėjos mokėjimo kortelę prie *Apple Pay* sistemos naujame įrenginyje, turėjo būti suvesti teisingi šios mokėjimo kortelės duomenys (įskaitant

---

[6] Jo telefono numerį, pareiškėjos teigimu, jos telefonas identifikavo kaip banko telefono numerį.

[7] „Skambintojo ID klastojimas" yra vienas iš sukčiavimo būdų. Tai praktika, kai telefono tinklas praneša skambučio gavėjui, kad skambučio iniciatorius yra kita stotis, o ne tikroji stotis. Dėl to skambintojo ID ekrane gali būti rodomas kitoks nei telefono, iš kurio buvo skambinta, telefono numeris (žr. https://en.wikipedia.org/wiki/Caller_ID_spoofing).

mokėjimo kortelės saugos kodą CVV) ir vienkartinis saugos kodas, kuris, banko Lietuvos bankui pateiktais duomenimis, buvo išsiųstas SMS žinute pareiškėjos telefono numeriu. Ginčo bylos duomenimis, kartu su vienkartiniu saugos kodu pareiškėjai SMS žinutėje buvo nurodyta šio kodo paskirtis ir perspėjimas jo neperduoti tretiesiems asmenims (standartinis siunčiamos SMS žinutės tekstas lietuvių kalba: „Šis kodas bus naudojamas jūsų kortelei pridėti prie kito Apple Pay įrenginio. Niekur jo neįveskite, nebent norite pridėti savo kortelę prie naujo įrenginio. Nesidalinkite šiuo kodu su niekuo, net jei jie teigia esantys iš Revolut. „Revolut" patvirtinimo kodas, skirtas „Apple Pay": xxxxxx")[8]. Suvedus gautą vienkartinį saugos kodą, mokėjimo kortelės pridėjimas buvo patvirtintas, o atsiskaitymo *Apple Pay* paslauga aktyvuota – ja naudojantis ir inicijuoti bei patvirtinti visi Ginčijami mokėjimai.

Informacijos, kokiam tikslui skirtas pareiškėjai SMS žinute atsiųstas vienkartinis saugos kodas, pareiškėja galėjo nematyti tik dėl to, kad buvo itin neatidi, neperskaičiusi žinutės teksto, pasitikėjo nepažįstamų jai skambinusių asmenų nurodymais ir atskleidė jiems šį kodą. Jeigu pareiškėja perskaitė SMS žinutės tekstą, tačiau jame nurodytą vienkartinį saugos kodą vis tiek nusprendė atskleisti tretiesiems asmenims, ji taip pat vertintina kaip elgusis itin aplaidžiai – nesuabejojusi, nepatikrinusi skambinusių asmenų ir jų nurodymų patikimumo ir galimo prieštaravimo tarp gautų nurodymų bei gautos SMS žinutės teksto, atskleidė vienkartinį saugos kodą tretiesiems asmenims ir šie veiksmai, taip pat mokėjimo kortelės duomenų atskleidimas įgalino trečiuosius asmenis tiek susieti pareiškėjos mokėjimo kortelę su *Apple Pay* mokėjimo metodu, tiek įvykdyti Ginčijamus mokėjimus.

Tai reiškia, kad Ginčijamus mokėjimus tretieji asmenys be pareiškėjos žinios galėjo atlikti tik dėl to, kad pareiškėja, būdama labai neatsargi, netinkamai vykdė Mokėjimų įstatymo (34 straipsnis) ir privatiems klientams taikomose sąlygose įtvirtintus mokėjimo kortelės saugaus naudojimo reikalavimus. Taigi, labiausiai tikėtina, kad būtent pareiškėja dėl didelio neatsargumo neišsaugojo jos vardu išduotos mokėjimo kortelės duomenų konfidencialumo, t. y. nesiėmė tų saugumo priemonių, kurių privalėjo imtis, kad būtų tinkamai apsaugoti jai suteiktos mokėjimo kortelės duomenys, ir tretiesiems asmenims suteikė (nurodė) vienkartinį saugos kodą, kurį gavo į jai priklausantį telefono numerį trumpąja SMS žinute, nors ta pačia SMS žinute buvo papildomai įspėta apie būtinybę niekam neatskleisti atsiųsto saugos kodo ir jį saugoti.

Konstatavus, kad pareiškėja, nesilaikydama jai, kaip mokėtojai, Mokėjimų įstatyme ir bendrojoje sutartyje su banku nustatytų pareigų, susijusių su išduotomis mokėjimo priemonėmis, elgėsi labai neatsargiai, darytina išvada, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, nustatančią, kad tokiu atveju mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai. Dėl to, Lietuvos banko vertinimu, bankas neprivalo grąžinti (kompensuoti) pareiškėjai neautorizuotų Ginčijamų mokėjimų lėšų ir pareiškėjos reikalavimas, kad bankas grąžintų pareiškėjai Ginčijamų mokėjimų lėšas – 2 148 GBP, atmestinas kaip nepagrįstas.

3. Dėl banko teikiamų paslaugų saugumo

Pagrįsdama bankui keliamą reikalavimą, pareiškėja kreipimesi taip pat teigia, kad bankas nesiėmė pakankamai priemonių tam, kad apsaugotų jos banko sąskaitoje esančias lėšas, be to, bankas nėra įsidiegęs pakankamai priemonių tam, kad stebėtų ir apsaugotų savo klientus nuo nesąžiningų mokėjimo operacijų.

Pažymėtina, kad finansų rinkos dalyviai, tarp jų ir bankas, teikdami finansines paslaugas, turi veikti profesionaliai ir skaidriai. Bankui, kaip profesionaliam verslininkui ir savo srities specialistui, yra keliami aukštesni profesionalumo, atidumo ir rūpestingumo standartai, todėl, turėdamas specifinių finansinių paslaugų teikimo srities žinių, bankas turėtų dėti visas reikiamas bei protingai įmanomas pastangas (įskaitant ir tinkamų prevencinių priemonių, teikiant mokėjimo paslaugas, įdiegimą) tam, kad klientai būtų kuo geriau apsaugoti nuo neautorizuotų ir (ar) nesąžiningų mokėjimo operacijų ir turėtų visas galimybes ginčijamų mokėjimo operacijų lėšas bandyti susigrąžinti, ypač sukčiavimų elektroninėje erdvėje atvejais[9].

[8] Tekstas anglų k.: „This code will be used to add your card to another Apple pay device. Don't enter it anywhere unless you want to add your card to a new device. Don't share this code with anyone, even if they claim to be from Revolut. Revolut verification code for Apple pay: xxxxxx."

[9] Tai, kad verslininkui, šiuo atveju ir bankui, kaip ir bet kuriam kitam savo srities profesionalui, teikiančiam paslaugas, teisės aktai nustato aukštesnį profesionalo teisėto elgesio standartą, taigi, kad jam taikomi aukštesni profesionalumo, atidumo ir rūpestingumo standartai, savo praktikoje ne kartą yra pabrėžęs ir kasacinis teismas. Pavyzdžiui, Lietuvos Aukščiausiojo Teismo 2008 m. vasario 28 d. nutartis civilinėje byloje Nr. 3K-3-112/2008; 2010 m. kovo 1 d. nutartis

Pateiktuose paaiškinimuose dėl teikiamų mokėjimo paslaugų saugumo ir klientų atliekamų mokėjimo operacijų stebėsenos bankas nurodė, kad mokėjimo operacijos kortele yra stebimos gyvai banko automatizuotos saugumo sistemos, kuri, veikdama autonomiškai pagal tam tikras nustatytas „taisykles" (kompiuterinius algoritmus), atlieka potencialios sukčiavimo rizikos vertinimą kiekvienos mokėjimo operacijos kortele atžvilgiu. Identifikavusi įtartinos kilmės mokėjimo operacijas kortele, toliau automatizuota saugumo sistema imasi šių veiksmų: mokėjimo operacijos atšaukimo, vėliau – mokėjimo kortelės užblokavimo ir kliento informavimo per banko mobiliąją programėlę bei elektroniniu paštu apie atšauktą mokėjimo operaciją ir užblokuotą mokėjimo kortelę.

Bankas paaiškino, kad banko įdiegta automatizuota saugumo sistema, prieš priimdama sprendimą vertinti mokėjimo operaciją kaip įtartiną, atsižvelgia į mokėjimo operacijos savybes (pavyzdžiui, naudos gavėjo informacija, suma, paros laikas); kliento ypatybes, t. y. palygina konkrečios mokėjimo operacijos reikšmę (ekonominė paskirtis) su mokėjimo operacijų istorija; naudos gavėjo ir prekybininko kategoriją, t. y. palygina inicijuojamą mokėjimo operaciją su visomis praeityje inicijuotomis įtartinomis ir neįtartinomis mokėjimo operacijomis nurodytam naudos gavėjui arba prekybininkui.

Šiuo atveju, kaip teigia bankas, analizuojant pareiškėjos mokėjimo operacijų istoriją, matyti, kad didžioji dalis pareiškėjos inicijuotų mokėjimo operacijų atspindi kasdienines reikmes bei asmeninio pobūdžio išlaidas – yra tiek didelės vertės mokėjimų, tiek ir labai mažos vertės mokėjimo operacijų. Ginčijami mokėjimai pagal sumą, palyginti su pareiškėjos praeityje inicijuotomis mokėjimo operacijos, niekuo neišsiskyrė, o Ginčijamų mokėjimų lėšų gavėjų (*Argos* ir *Sainsburys Supermarket*) naudai praeityje pati pareiškėja yra atlikusi mokėjimo operacijų.

Bankas nurodė, kad pareiškėjai paskambinęs tariamas banko darbuotojas po įvykdytų Ginčijamų mokėjimų mėgino inicijuoti dar vieną 250 GBP (290,49 Eur) vertės mokėjimą kortele naudos gavėjui *Sainsburys Supermarket*. Ši mokėjimo operacija buvo atšaukta banko automatizuotos saugumo sistemos kaip įtartina, o pareiškėjos mokėjimo kortelė užblokuota. Pareiškėja apie tokį banko automatizuotos saugumo sistemos veiksmą ir potencialią sukčiavimo riziką buvo informuota tiek per banko programėlę savo mobiliajame įrenginyje, tiek elektroniniu paštu, kuris yra susietas su jos mokėjimo sąskaita.

Kaip minėta, nagrinėdamas ginčus Lietuvos bankas neatlieka patikrinimų tam, kad nustatytų, ar nebuvo pažeisti finansų įstaigų veiklai keliami teisės aktų reikalavimai. Lietuvos bankas remiasi ginčo šalių pateiktais konkrečiais įrodymais, kurių pagrindu priima sprendimą. Atsižvelgiant į tai, darytina išvada, kad ginčo byloje nėra jokių duomenų, galinčių patvirtinti pareiškėjos nurodytą aplinkybę, kad bankas nesiėmė reikiamų veiksmų, kad apsaugotų pareiškėjos banko sąskaitose esančias lėšas, o įvykdydamas Ginčijamus mokėjimus būtų pažeidęs finansų rinką reglamentuojančių teisės aktų reikalavimus. Priešingai, bankas pateikė konkrečius duomenis, kad banko automatizuotos saugumo (mokėjimo operacijų stebėsenos) sistemos šiuo atveju buvo veiksmingos ir paskutinę trečiųjų asmenų inicijuotą mokėjimo operaciją mokėjimo kortele (panaudojant *Apple Pay* mokėjimo metodą) atšaukė ir pareiškėjos mokėjimo kortelę užblokavo.

Verta atkreipti dėmesį ir į tai, kad faktas, jog, vykdydama trečiųjų asmenų apgaulingus nurodymus, pareiškėja sudarė sąlygas savo mokėjimo kortelę pridėti prie *Apple Pay* įrenginio ir įvykdyti visus Ginčijamus mokėjimus, savaime nereiškia, kad bankas nesilaikė teisės aktų reikalavimų, susijusių su lėšų mokėjimo kortelės sąskaitoje saugumo užtikrinimu. Aplinkybė, kad Ginčijami mokėjimai buvo įvykdyti dėl trečiųjų asmenų apgaulingų ir neteisėtų veiksmų paaiškėjo jau vėliau, kai Ginčijami mokėjimai jau buvo įvykdyti, o mokėjimo kortelė užblokuota apie tai pačiai pareiškėjai informavus banką.

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.

---

civilinėje byloje Nr. 3K-3-69/2010; 2018 m. spalio 12 d. nutartis civilinėje byloje Nr. e3K-3-60-969/2018.

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. 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