LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

SPRENDIMAS DĖL X. X. IR BANKO *LUMINOR BANK AS* GINČO NAGRINĖJIMO

2023-09-22 Nr. 429-480
Vilnius

Lietuvos bankas gavo X. X. (toliau – pareiškėjas) kreipimąsi, kuriuo prašoma išnagrinėti tarp pareiškėjo ir banko *Luminor Bank AS*, veikiančio per skyrių Lietuvoje, (toliau – bankas) kilusį ginčą.

N u s t a t y t a:

2023 m. balandžio 17 d. iš pareiškėjo atsiskaitomosios sąskaitos buvo atlikta 690 Eur mokėjimo operacija gavėjai Y. Y. (toliau – Operacija).

Tą pačią dieną 16 val. 13 min. pareiškėjas kreipėsi telefonu į banką ir pranešė, kad iš Valstybinės mokesčių inspekcijos (toliau – VMI) gavo SMS pranešimą, kuriuo buvo informuotas apie jam paskirtą administracinę nuobaudą, SMS pranešime buvo aktyvi nuoroda, ją paspaudęs pareiškėjas galėjo neva susipažinti su pranešimu. Pareiškėjas teigia paspaudęs aktyvią nuorodą, atsidariusiame interneto puslapyje suvedęs prisijungimo prie banko interneto banko aplinkos duomenis, taip pat „Smart-ID" paskyros PIN1 ir PIN2 kodus. Suvedęs kodus pareiškėjas pastebėjo jo sąskaitoje įvykdytą jo neautorizuotą Operaciją.

Pokalbio metu pareiškėjui teikiama interneto banko paslauga buvo užblokuota, padedamas banko darbuotojo pareiškėjas per interneto banką užpildė Prašymą atšaukti pervedimą.

Atsižvelgdamas į pareiškėjo pateiktus duomenis, bankas nustatė, kad nėra techninių galimybių atšaukti Operaciją. Iš pateiktų duomenų matyti, kad bankas papildomai inicijavo Operacijos atšaukimą pagal pareiškėjo pateiktą prašymą, tačiau iš lėšų gavėjo mokėjimo paslaugų teikėjo gavo atsakymą, jog lėšų likutis lėšų gavėjo sąskaitoje yra nepakankamas grąžinimui atlikti.

Remdamasis visa surinkta informacija, bankas priėmė sprendimą atsisakyti pareiškėjui atlyginti jo patirtus nuostolius, nes nustatė, kad pareiškėjas pats, būdamas labai neatsargus, patvirtino Operaciją.

2023 m. birželio 6 d. pareiškėjas kreipėsi į banką ir prašė pakartotinai apsvarstyti priimtą sprendimą, tačiau 2023 m. birželio 20 d. bankas pareiškėjui pateikė atsakymą, kad priimtas sprendimas yra pagrįstas ir keičiamas nebus. Pareiškėjas su tuo nesutiko, todėl tarp šalių kilo ginčas.

Kreipimesi į Lietuvos banką pareiškėjas prašo įpareigoti banką grąžinti Operacijos metu iš pareiškėjo atsiskaitomosios sąskaitos nurašytas lėšas, t. y. 690 Eur. Pareiškėjas Lietuvos bankui nurodė analogiškas aplinkybes kaip ir kreipimesi į banką. Pareiškėjas papildomai pažymėjo, kad po sukčiavimo atakos bandė susisiekti su banku, tačiau iš karto niekas neatsiliepė į pareiškėjo skambutį, o po to, kai pavyko susisiekti, prašė sustabdyti Operaciją arba atlikti kitus veiksmus, galinčius užkirsti kelią lėšų nuskaitymui, tačiau bankas nesiėmė jokių veiksmų, kurių pagrindu būtų galima atšaukti Operaciją.

Atsiliepime į pareiškėjo kreipimąsi bankas nurodo nesutinkąs su pareiškėjo reikalavimu ir prašo jį atmesti. Bankas nurodo, kad Operacija buvo tinkamai autorizuota pareiškėjo sutartyje nustatyta tvarka, t. y. jis pats suvedė tik jam vienam žinomus personalizuotus saugumo duomenis. Dėl šios priežasties pagal teisės aktų nuostatas bankas negali būti atsakingas už tinkamai ir teisingai autorizuotų mokėjimo operacijų įvykdymą.

Banko teigimu, net jeigu būtų pripažinta, kad Operacija buvo neautorizuota, vis dėlto pareiškėjui buvo sudarytos visos sąlygos susipažinti su Operacijos detalėmis ir jos nepatvirtini.

Taigi, banko teigimu, pareiškėjo veiksmai vienareikšmiškai laikytini kaip labai neatsargūs. Bankas nurodo, kad pareiškėjas nesilaikė šalių sudarytos sutarties nuostatų ir aktyviais savo veiksmais tretiesiems asmenims atskleidė personalizuotus saugumo duomenis. Pareiškėjui atsiųstas SMS pranešimas akivaizdžiai buvo siųstas ne VMI, o nuoroda, kurią pareiškėjas paspaudė, buvo kitokia, nei naudoja institucija. Be to, suklastota banko svetainė, į kurią buvo nukreiptas pareiškėjas, tiek struktūra, tiek vizualiai neatitiko originalaus banko puslapio išdėstymo, o tam tikri mygtukai, susiję su produktais, kalbos keitimu ir pan., neveikė. Kadangi pareiškėjo atliekami veiksmai nevedė prie tariamos informacijos apie gautą administracinę nuobaudą, tai pareiškėjui turėjo sukelti abejonių dėl veiksmų tinkamumo.

Banko teigimu, pareiškėjas atsidariusiame suklastotame banko interneto banko puslapyje pateikė savo asmeninius prisijungimo prie interneto banko duomenis, tada savo išmaniajame įrenginyje suvedė tik pareiškėjui žinomą „Smart-ID" paskyros PIN1 kodą, o Operacijai patvirtinti ir „Smart-ID" paskyros PIN2 kodą. Prieš patvirtindamas Operaciją pareiškėjas turėjo matyti tiek tvirtinamos Operacijos sumą, tiek kontrolinį kodą, todėl jam turėjo kilti įtarimų ir jis galėjo nepatvirtinti Operacijos. Taigi, banko teigimu, pareiškėjas nepatikrino tvirtinamos Operacijos (Operacijos sumos) ir kontrolinių kodų, todėl buvo labai neatsargus.

Banko teigimu, pareiškėjas turėjo galimybę atkreipti dėmesį į netikro tinklalapio, kuris atsidarė pareiškėjui paspaudus aktyvią nuorodą, adresą. Bankas pirmiausia rekomenduoja klientams įvertinti, ar SMS pranešimuose, el. paštu ar kitais kanalais gautos nuorodos atidaro tikras, o ne suklastotas pardavėjo ar paslaugų teikėjo interneto svetaines, kurių vardu tokios nuorodos siunčiamos. Tai, banko teigimu, viena iš pagrindinių banko nurodytų saugaus elgesio internete vykdant finansines operacijas taisyklių, kurias bankas yra paskelbęs savo interneto svetainėje.

Banko teigimu, apie sukčių vykdomas atakas ir bandymus išvilioti lėšas bankas nuolatos skelbia žiniasklaidoje, spaudoje, radijuje ir kitomis priemonėmis. Bankas reguliariai savo interneto puslapyje įspėja klientus apie sukčiavimo atvejus, dar kovo mėnesį įspėjo klientus apie suaktyvėjusį suklastotų žinučių siuntimą, o pareiškėjo nurodytu el. pašto adresu 2023 m. vasario 15 d. ir 2023 m. gegužės 23 d. siuntė el. laiškus su naudinga informacija, kaip apsisaugoti nuo sukčių.

Bankas nurodo ir tai, kad, pareiškėjui patvirtinus Operaciją, ji buvo įvykdyta kaip momentinis pavedimas, t. y. nedelsiant, o tokių mokėjimo operacijų atšaukti nėra galimybės, todėl šiuo atveju net jeigu pareiškėjas ir būtų kreipęsis į banką dar anksčiau, vis tiek nebūtų buvusios galimybės atšaukti Operacijos.

Dėl šių priežasčių, remdamasis atsiliepime išdėstytais argumentais, bankas nurodo, kad Operacija turi būti laikoma autorizuota. Jeigu Operacija bus laikoma neautorizuota, tokiu atveju pareiškėjo elgesys buvo labai neatsargus, visi nuostoliai pagal teisės aktų nuostatas turėtų tekti pačiam pareiškėjui, todėl bankas prašo atmesti pareiškėjo reikalavimą kaip nepagrįstą.

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

Vadovaujantis Lietuvos banko valdybos 2012 m. sausio 26 d. nutarimu Nr. 03-23 patvirtintų Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių 45 punktu, vartojimo ginčai Lietuvos banke nagrinėjami laikantis rungimosi, ginčų nagrinėjimo operatyvumo, koncentracijos, ekonomiškumo ir bendradarbiavimo principų. 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. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Pareiškėjo ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjui Operacijos metu iš jo atsiskaitomosios sąskaitos pervestą sumą. Pareiškėjas neigia autorizavęs Operaciją, todėl mano, kad bankas šio mokėjimo lėšas turi grąžinti pareiškėjui. Banko vertinimu, Operacija laikytina tinkamai autorizuota – pats pareiškėjas iš savo įrenginio patvirtino Operaciją, suvesdamas „Smart-ID" paskyros PIN1 ir PIN2 kodus. Atsižvelgdamas ir į tai, kad, banko teigimu, pareiškėjo veiksmams būdingas didelis neatsargumas, bankas mano, kad negali būti įpareigotas Operacijos sumos grąžinti pareiškėjui.

Siekdamas išspręsti tarp šalių kilusį ginčą ir įvertinti pareiškėjo bankui keliamo reikalavimo pagrįstumą, Lietuvos bankas vertins, ar: 1) Operacija laikytina autorizuota; 2) atsisakydamas grąžinti pareiškėjui Operacijos metu pervestas lėšas, bankas pagrįstai rėmėsi Mokėjimų įstatymo 39 straipsnio 3 dalimi; 2) bankas pagrįstai nesustabdė ir (ar) neatšaukė Operacijos vykdymo.

1. Dėl Operacijos autorizavimo

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.

Mokėjimų įstatymo 29 straipsnio 1 dalyje nustatyta, kad mokėjimo operacija laikoma autorizuota tik tada, kai mokėtojas duoda sutikimą įvykdyti mokėjimo operaciją. Jeigu mokėtojo sutikimo įvykdyti mokėjimo operaciją nėra, laikoma, kad mokėjimo operacija yra neautorizuota (Mokėjimų įstatymo 29 straipsnio 2 dalis).

Mokėjimų 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.

Banko mokėjimo paslaugų teikimo sąlygų 11.9 papunktyje nustatyta, kad „mokėjimo operacija laikoma autorizuota tik tada, kai Klientas duoda sutikimą ją vykdyti. Šio sutikimo davimo forma ir tvarka nustatoma sutartyje. Klientas gali autorizuoti mokėjimo operaciją iki jos įvykdymo arba ją įvykdęs, jeigu taip susitarė Klientas ir Bankas. Jeigu pirmiau nurodyto sutikimo nėra, laikoma, kad mokėjimo operacija yra neautorizuota.“ Vadovaujantis banko mokėjimo paslaugų teikimo sąlygų 6.3.1 papunkčio, nurodančio, kokiais būdais banko klientas gali pateikti sutikimą atlikti operaciją, nuostatomis, „Klientas sutikimą atlikti mokėjimo operaciją gali pateikti Banko nustatyta arba Banko ir Kliento sutarta forma ir būdu.<...> Sutikimas dėl mokėjimo operacijų taip pat gali būti tvirtinamas naudojant Kliento atpažinimo priemones ir / ar kitais Bankui priimtinais būdais / priemonėmis.“

Nors pirmiau aptartomis banko mokėjimo paslaugų teikimo sąlygų nuostatomis bankas remiasi, grįsdamas teiginį, kad Operacija buvo tinkamai, t. y. šalių sutartu būdu, autorizuota, būtina pažymėti, kad minėtose nuostatose kalbama apie atvejus, kai mokėtojas duoda savo sutikimą pervesti lėšas ir tuo tikslu panaudoja jam išduotas mokėjimo ir tapatybės patvirtinimo priemones. Vis dėlto nagrinėjamo ginčo atveju, priešingai, nei nurodyta aptariamose nuostatose, pareiškėjas savo personalizuotus saugumo duomenis panaudojo fiktyvioje – paspaudus SMS žinute gautą nuorodą atsiradusioje, interneto svetainėje ir juos suvedė ne dėl to, kad ketino atlikti konkrečią Operaciją trečiajam asmeniui, o vykdydamas gautoje žinutėje pateiktus nurodymus ir siekdamas peržiūrėti pranešimą apie jam paskirtą administracinę nuobaudą bei ją sumokėti. Pareiškėjas tiek bendraudamas su banku dėl Operacijos, tiek ir kreipimesi į Lietuvos banką nuosekliai laikosi pozicijos, kad valios inicijuoti ir įvykdyti Operaciją jis neišreiškė ir nedavė tam savo sutikimo.

Bankas kartu su atsiliepimu pateikė jo vidaus sistemose užfiksuotus duomenis, pagrindžiančius, kad Operacijai inicijuoti buvo suvesti pareiškėjo personalizuoti saugumo duomenys, tai buvo patvirtinta „Smart-ID“ paskyros PIN1 kodu, o Operacijai patvirtinti buvo suvestas ir „Smart-ID“ paskyros PIN2 kodas.

Taigi, bankas, darydamas išvadą, kad Operacija buvo autorizuota šalių sutarta tvarka, iš esmės remiasi tik tuo faktu, kad, banko vidinės sistemos duomenimis, Operacijai įvykdyti buvo panaudoti tik pareiškėjui žinomi personalizuoti saugumo duomenys, suvesti pareiškėjo „Smart-ID“ paskyros PIN1 ir PIN2 kodai ir kad visi veiksmai buvo atlikti iš pareiškėjo įrenginio. Tačiau svarbu yra tai, kad, darydamas tokią išvadą, bankas nevertino, kuriuo metu, kaip ir kieno iniciatyva buvo inicijuota Operacija, t. y. ar šiuo atveju pats pareiškėjas siekė atlikti Operaciją, ar ją siekė atlikti neteisėtai iš pareiškėjo duomenis išvilioję tretieji asmenys.

Vis dėlto, Lietuvos banko vertinimu, vien šie duomenys dar savaime neįrodo, kad Operacija iš tiesų atlikta esant pareiškėjo sutikimui (pareiškėjo valia ir su jo sutikimu). Kaip minėta pirmiau, remiantis Mokėjimų įstatymo nuostatomis, vien aplinkybė, kad mokėtojo mokėjimo paslaugų teikėjo vidaus sistemose užregistruotas mokėtojui išduotos mokėjimo priemonės, įskaitant jos personalizuotus saugumo duomenis, naudojimas, nebūtinai yra pakankamas įrodymas, jog mokėjimo priemone naudojosi ir (arba) mokėjimo operaciją autorizavo pats mokėtojas (Mokėjimų įstatymo 37 straipsnio 3 dalis).

Lietuvos banko nuomone, sprendžiant, ar Operacija laikytina autorizuota, būtina nustatyti, ar faktinės Operacijos patvirtinimo aplinkybės, kurias pagrindžia ginčo byloje esantys

duomenys, atitiko ginčo šalių sudarytoje sutartyje aptartą mokėjimo operacijų autorizavimo tvarką. Taigi, ar pareiškėjas, suklastotoje interneto svetainėje pateikdamas tam tikrus personalizuotus saugumo duomenis ir tikėdamasis, kad tokiu būdu patikrins jam paskirtą administracinės nuobaudos pranešimą ir sumokės baudą, suprato, kad iš tiesų atlieka veiksmus, kurie vėliau gali lemti lėšų nurašymą iš jo sąskaitos.

Pareiškėjas, pagrįsdamas teiginį, kad nesiekė Operacijos inicijavimo ir jos neautorizavo, pateikė jam atsiųsto SMS pranešimo, kuriame matyti, kad pareiškėjas buvo raginamas paspausti nuorodą ir susipažinti su jam išsiųstu pranešimu apie paskirtą administracinę nuobaudą, kopiją. Kaip matyti iš pareiškėjo pateikto SMS pranešimo kopijos, jam buvo pateikta nuoroda į suklastotą VMI interneto svetainę, atsidariusiame puslapyje pareiškėjas turėjo pasirinkti jo naudojamą banką, o vėliau suklastotame banko puslapyje pareiškėjas turėjo atlikti prisijungimo prie interneto banko aplinkos veiksmus.

Nurodytos aplinkybės leidžia teigti, kad SMS pranešime pateikta informacija, taip pat galimai ir pagal nuorodą atsidariusiame interneto puslapyje, o vėliau ir suklastotame banko puslapyje nurodyti duomenys bei matomi vaizdai galėjo pareiškėjui sukurti pirminį įspūdį, kad pareiškėjas prisijungia prie VMI aplinkos, kurioje bus galima patikrinti pranešimą apie jam paskirtą administracinę nuobaudą ir už ją sumokėti.

Norėdamas pagrįsti savo poziciją, kad Operacija buvo tinkamai autorizuota, bankas, be kita ko, nurodo, kad, identifikacijai pasirinkus „Smart-ID" programėlę, mokėjimo paslaugų naudotojas yra nustatomas naudojantis šios tapatybės patvirtinimo priemonės paskyros PIN1 kodu: tokiais atvejais „Smart-ID" programėlėje yra rodomas operacijos kontrolinis kodas, kuris turi sutapti su kontroliniu kodu, kurį mokėtojas mato banko autentifikavimo lange. Todėl pareiškėjas tik patikrinęs kontrolinio kodo atitiktį turėjo suvesti „Smart-ID" paskyros PIN1 kodą. Bankas paaiškino, kad jeigu klientai siekia atlikti mokėjimo operaciją, tokiu atveju pakartotinai „Smart-ID" programėlėje yra rodomas operacijos kontrolinis kodas, kuris turi sutapti su kontroliniu kodu, kurį mokėtojas mato banko autentifikavimo lange, o „Smart-ID" programėlėje yra rodoma tvirtinamos Operacijos suma. Banko teigimu, jeigu nėra galimybės sutikrinti kontrolinių kodų arba pateikta Operacijos suma yra nežinoma, tokiu atveju klientas neturi tvirtinti savo tapatybės arba tvirtinti tokios Operacijos.

Vis dėlto, remiantis banko paaiškinimais, be kontrolinio kodo ir tvirtinamos Operacijos sumos, kuriuos turi sutikrinti mokėtojas, nėra atliekami jokie kiti veiksmai ir mokėtojui, be banko interneto banke operacijos lange nurodytų duomenų, papildomai nėra rodoma jokia informacija, susijusi su inicijuota mokėjimo operacija. Jeigu mokėtojas pasirinko programėlę „Smart ID" kaip tapatybės patvirtinimo priemonę, pasirodžiusiame pranešime, kuriuo operacijai patvirtinti prašoma suvesti „Smart ID" paskyros PIN2 kodą, mokėtojui nėra rodoma jokia papildoma informacija, t. y. lėšų gavėjas, paaiškinamas atliekamas veiksmas ir pan. Tokiu atveju (tvirtinant mokėjimą, inicijuotą kaip kredito pervedimas) mokėtojui nėra rodoma papildoma informacija, kuri leistų papildomai susipažinti su visa atliekamų mokėjimo operacijų informacija ir ją įvertinti.

Būtina atkreipti dėmesį į tai, kad, nustatytomis aplinkybėmis, Operacijai inicijuoti būtini duomenys buvo suvesti suklastotoje interneto svetainėje, kurioje pareiškėjui buvo rodoma informacija apie prisijungimą prie VMI aplinkos per banko interneto banko paskyrą. Dėl šios priežasties ginčo byloje nėra jokių duomenų, kurie galėtų patvirtinti, kad pareiškėjas, duomenis, būtinus Operacijai inicijuoti ir patvirtinti, suvedęs suklastotoje interneto svetainėje, turėjo ir galėjo suvokti, kad šiuo metu ne tvirtina savo tapatybę tam, kad galėtų sumokėti administracinę baudą arba ją moka administracinę nuobaudą, o lėšas perveda trečiajam asmeniui ne savo valia.

Vadinasi, ginčo byloje esantys įrodymai, tarp jų ir pirmiau aptarti duomenys dėl Operacijos inicijavimo ir įvykdymo aplinkybių, kurių nepaneigė banko paaiškinimai ir pateikti vidinės sistemos duomenys apie tai, kad Operacijai patvirtinti panaudoti pareiškėjo personalizuoti saugumo duomenys ir suvesti pareiškėjo naudojamos „Smart-ID" paskyros PIN1 ir PIN2 kodai, Lietuvos banko vertinimu, leidžia pagrįstai daryti išvadą, kad trečiųjų asmenų sukurtoje aplinkoje pareiškėjui rodoma informacija pagrįstai galėjo suklaidinti ir pareiškėjas galėjo tikėtis, kad jungiamasi prie VMI aplinkos arba mokama administracinė bauda. Vadinasi, duomenų, jog pareiškėjas žinojo, suprato ir išreiškė savo valią inicijuoti ir autorizuoti Operaciją šalių sutarta tvarka, nagrinėjamu atveju nėra.

Atsižvelgiant į tai, Lietuvos banko nuomone, vertinti Operaciją kaip autorizuotą – atliktą esant paties pareiškėjo sutikimui (kaip tai suprantama Mokėjimų įstatymo 29 straipsnio 1 dalies kontekste), nors jis ir atitiko pareiškėjo ir banko sutartą sutikimo vykdyti mokėjimo operacijas

davimo formą ir tvarką, nėra pagrindo, todėl Lietuvos bankas daro išvadą, kad Operacija laikytina neautorizuota.

2. Dėl Mokėjimų įstatymo 39 straipsnio 3 dalies taikymo

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.

Duomenų, kad nagrinėjamu atveju pareiškėjas galėjo veikti nesąžiningai arba tyčia, nėra, todėl galimas mokėtojo sukčiavimas, kaip pagrindas atleisti mokėtojo mokėjimo paslaugų teikėją nuo pareigos atlyginti mokėtojui nuostolius dėl neautorizuotos mokėjimo operacijos įvykdymo, šiame sprendime atskirai nebus plačiau analizuojamas.

Taigi, sprendžiant, ar banko atsisakymas grąžinti pareiškėjui Operacijos sumą laikytinas pagrįstu, būtina įvertinti, ar pareiškėjo elgesys, atskleidžiant tretiesiems asmenims personalizuotus saugumo duomenis, vertintinas kaip didelis neatsargumas, dėl kurio su mokėjimo operacijos įvykdymu atsiradę nuostoliai, kaip nustatyta Mokėjimų įstatymo 39 straipsnio 3 dalyje, tektų pačiam pareiškėjui.

Lietuvos Aukščiausiasis Teismas yra išaiškinęs, kad didelis neatsargumas pasireiškia neprotingu arba išskirtiniu rūpestingumo nebuvimu, kai asmuo nėra tiek rūpestingas, kiek akivaizdžiai būtina esamomis aplinkybėmis[1].

Dėl mokėtojo neatsargumo laipsnio vertinimo, pagrindinių jo kriterijų ir glaudaus ryšio su ginčo byloje nustatytų individualių specifinių aplinkybių visuma Lietuvos bankas yra ne kartą plačiau pasisakęs savo ginčų nagrinėjimo praktikoje[2], todėl šiame sprendime bus pasisakoma tik šiai konkrečiai ginčo bylai aktualiais aspektais.

Neautorizuotos mokėjimo operacijos įvykdymo atveju didelis neatsargumas yra sietinas su vienos ar kelių Mokėjimų įstatymo 34 straipsnyje mokėtojui nustatytų pareigų, susijusių su mokėjimo priemone ir personalizuotais saugumo duomenimis, nevykdymu.

Mokėjimų įstatymo 34 straipsnis nustato mokėtojo pareigą naudotis jam išduota mokėjimo priemone (nagrinėjamu atveju – mokėjimo kortele) 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 pareigą, gavus mokėjimo priemonę, imtis veiksmų, kad būtų apsaugoti personalizuoti saugumo duomenys (Mokėjimų įstatymo 34 straipsnio 2 dalis).

Panašios pareigos nustatytos banko ir pareiškėjo bendrąją sutartį sudarančių Banko mokėjimo paslaugų teikimo sąlygų 7.3.1 papunktyje: „interneto banke vykdomos mokėjimo operacijos autorizuojamos naudojant Kliento atpažinimo priemones, kurias Klientas / Sąskaitos valdytojas privalo saugoti šiose mokėjimo paslaugų teikimo sąlygose nustatyta tvarka. Tokiu būdu patvirtinti dokumentai, laikomi patvirtintais Kliento ir turinčiais tokią pat teisinę galią, kaip ir Kliento ar jo atstovo pasirašyti popieriniai dokumentai.“ Tų pačių sąlygų 7.3.4 papunktyje yra įtvirtina, kad „Klientas / Sąskaitų valdytojas privalo užtikrinti jam patikėtų Kliento atpažinimo priemonių saugumą: neturi teisės jų perduoti nei kitam asmeniui, nei kitam Sąskaitos valdytojui, nei bet kokiam kitam Kliento atstovui; įsipareigoja laikyti juos paslaptyje, nerašyti jų ant popieriaus, ant kitokių daiktų bei laikyti kitokiame, išskyrus Banko suteiktame, pavidale“, o 9.2 papunktyje įtvirtinta kliento, turinčio teisę naudotis mokėjimo priemone, pareiga: „Klientas, gavęs mokėjimo priemonę, privalo imtis veiksmų, kad apsaugotų Personalizuotus saugumo duomenis.“

Taigi, pirmiau aptartos mokėjimo paslaugų sutarties (ją sudarančių dokumentų) nuostatos aiškiai nustato, kad už mokėjimo ir tapatybės patvirtinimo priemonių personalizuotų saugumo duomenų konfidencialumą yra atsakingas mokėtojas, šiuo atveju – pareiškėjas, jis privalo užtikrinti, kad minėti duomenys netaptų žinomi tretiesiems asmenims. Atsižvelgiant į tai, manytina, kad pareiškėjo elgesys būtų laikomas kaip atitinkantis mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, jei būtų nustatyta, kad pareiškėjas ėmėsi adekvačių veiksmų (arba priešingai – nustačius, kad nuo tam tikrų veiksmų susilaikė) tam, kad jam banko išduotų mokėjimo priemonių personalizuotų saugumo duomenų, įgalinančių inicijuoti

[1] Lietuvos Aukščiausiojo Teismo 2017 m. balandžio 13 d. nutartis civilinėje byloje Nr. e3K-3-180-378/2017.
[2] Pavyzdžiui, ginčo bylos Nr. 2022-00586 ir 2022-02496.

ir tvirtinti mokėjimus, konfidencialumas būtų tinkamai užtikrintas ir jie būtų naudojami šalių sutartinius santykius reglamentuojančių dokumentų nustatyta tvarka bei sąlygomis.

Vis dėlto, įvertinus ginčo byloje esančius duomenis ir ginčo nagrinėjimo metu nustatytas aplinkybes, išvados, kad pareiškėjo elgesys atitiko banko nustatytas naudojimosi mokėjimo priemonėmis sąlygas ir buvo adekvatus, pakankamas tam, kad pareiškėjui nustatytos pareigos, susijusios su mokėjimo priemonių personalizuotų saugumo duomenų konfidencialumo užtikrinimu, būtų tinkamai įvykdytos, daryti negalima.

Nors pareiškėjui atsiųstas SMS pranešimas galėjo sukurti pirmąjį įspūdį, kad šis pranešimas išsiųstas VMI, tačiau tai, kad pareiškėjas iki personalizuotų duomenų atskleidimo (pateikimo suklastotoje interneto svetainėje) nesudvejojo pranešime nurodytos informacijos ir jam nepažįstamo siuntėjo patikimumu, leidžia teigti, kad pareiškėjo elgesys inicijuojant Operaciją nebuvo itin apdairus ir atsargus.

Pažymėtina, kad pareiškėjas, gavęs SMS pranešimą, turėjo įvertinti SMS pranešimo siuntėją ir pranešimo turinį. SMS pranešimas buvo atsiųstas ne iš Lietuvoje, o iš užsienyje registruoto numerio[3], nors pranešimą neva siuntė Lietuvos institucija, be to, atsiųstas SMS pranešimas buvo parašytas be lietuviškų raidžių, o pats jo turinys skatino pareiškėją tik susipažinti su administracinės nuobaudos pranešimu, o ne sumokėti pačią administracinę baudą[4]. Pareiškėjas į šias aplinkybes neatkreipė dėmesio, paspaudė SMS pranešime pateiktą aktyvią nuorodą ir buvo nukreiptas į suklastotą VMI tinklalapį, kuriame, pasirinkęs pasirinktį, kad yra banko klientas, turėjo suvesti visus prisijungimui prie banko sąskaitos reikalingus duomenis, t. y. naudotojo ID ir asmens kodą. Taip tretieji asmenys įgijo galimybę inicijuoti prisijungimą prie tikrosios pareiškėjo banko interneto banko aplinkos.

Po šių veiksmų pareiškėjo „Smart-ID" programėlės ekrane pasirodė pranešimas, kad pareiškėjas jungiasi prie banko interneto banko aplinkos, todėl pareiškėjas suvedė „Smart-ID" paskyros PIN1 kodą, tai leido tretiesiems asmenims prisijungti prie tikrosios pareiškėjo banko interneto banko paskyros.

Svarbu ir tai, kad pareiškėjas neskyrė pakankamai dėmesio tam, kad tinkamai susipažintų su veiksmu, kurį jo prašoma patvirtinti, t. y. kad buvo prašoma patvirtinti Operaciją, ir nurodyta tvirtinama suma, t. y. 690 Eur. Pareiškėjui, nesusipažinus su administracinės nuobaudos pranešimu ir nežinant tikslios baudos sumos, turėjo kilti pagrįstų abejonių, kodėl prašoma patvirtinti būtent tokio dydžio sumą ir kodėl (už kokias tariamai nesumokėtas administracines baudas) yra atliekama Operacija.

Vis dėlto, vertinant pareiškėjo elgesį būtent nagrinėjamo ginčo aplinkybių ir prieš pareiškėją nukreiptos specifinės sukčiavimo atakos kontekste, esminėmis aplinkybėmis, vertinant pareiškėjo neatsargumo laipsnį, Lietuvos banko vertinimu, laikytina tai, kad pareiškėjui nesukėlė jokių įtarimų tai, kad SMS pranešimas yra atsiųstas iš užsienyje registruoto telefono numerio, nors suklastotą SMS pranešimą siunčia neva Lietuvos institucija. Be to, nors pareiškėjui SMS pranešime buvo nurodoma, kad jis paspaudęs aktyvią nuorodą turi tik susipažinti su administracinės nuobaudos pranešimu, pareiškėjas nedvejodamas ir nesusipažinęs su nurodytais pranešimais iš karto patvirtinto Operaciją.

Kaip minėta, pagal banko mokėjimo paslaugų teikimo sąlygas, personalizuotų saugumo duomenų pateikimas minėtose sąlygose numatytais atvejais laikomas kliento (šiuo atveju – pareiškėjo) sutikimu įvykdyti mokėjimo operaciją, lėšas nurašant iš kliento (šiuo atveju – pareiškėjo) sąskaitos. Atitinkamai ginčo byloje nėra jokių duomenų, kad pareiškėjas būtų kvestionavęs SMS pranešime nurodytą tekstą ir pateiktos nuorodos tikrumą, o jei tokių abejonių turėjo, nėra jokių duomenų, kad šias abejones būtų bandęs išsklaidyti, patikrinti gautą informaciją. Pareiškėjui nesukėlė įtarimų ir jam atsiųsto SMS pranešimo, kuris yra parašytas be lietuviškų raidžių, turinys bei tai, kad pranešime pateikta nuoroda skiriasi nuo VMI naudojamos interneto banko nuorodos (VMI oficiali nuoroda https://www.vmi.lt/evmi/, o trečiųjų asmenų SMS pranešime pateikta vmi.lt-v-prisijungti.net).

Banko viešai skelbiamose saugaus naudojimosi elektroninėmis paslaugomis rekomendacijose banko klientai raginami prisijungti prie banko paskyros tik per oficialų banko tinklalapį arba banko programėlę, jungiantis prie banko interneto banko įsitikinti, ar yra tinkamas banko interneto banko adresas, įvertinti svetainę, kurioje suveda personalizuotus saugumo duomenis, t. y. patikrinti, ar veikia visi mygtukai, ir pan. Taip pat bankas pateikė duomenis, kad 2023 m. kovo mėn. visus klientus įspėjo apie suaktyvėjusį suklastotų žinučių

[3] Telefono numeris, iš kurio buvo atsiųstas SMS pranešimas,yra +48572964928.
[4] SMS pranešimo tekstas: VMI: Del nesumoketu administraciniu baudu, mes issiunteme jusm pranesima. Prisijunkite cia: vmi.lt-v-prisijungti.net.

siuntimą[5]. Be to, pareiškėjas 2023 m. vasario 15 d. el. laišku asmeniškai buvo įspėtas, kad būtų budrus, nes sukčiai aktyviai vilioja bankų klientų duomenis.

Taigi, iš šių duomenų matyti, kad bankas, būdamas savo srities profesionalas, prevenciškai dėjo pastangas tam, kad pareiškėjas būtų supažindintas su sukčiavimo elektroninėje erdvėje rizikomis bei tapatybės patvirtinimo priemonės saugaus naudojimo, jos personalizuotų saugumo žymenų suvedimo ir atskleidimo reikšme bei teisinėmis pasekmėmis.

Iš banko pateiktų duomenų matyti, kad ir VMI nuo 2023 m. balandžio 11 d. aktyviai platino pranešimus, kuriuose skatino visus asmenis saugotis panašaus pobūdžio sukčiavimo atakų[6]. Taigi, pareiškėjas turėjo galimybę susipažinti ir su panašių sukčiavimo atakų pobūdžiu dar iki prieš pareiškėją nukreiptos sukčiavimo atakos.

Atsiliepime į pareiškėjo kreipimąsi bankas, siekdamas pagrįsti priimtą sprendimą, akcentavo, kad pareiškėjas turėjo galimybę įvertinti atsiųstas tinklalapių nuorodas ir pastebėti, kad jos yra netikros. Bankas teigia ne kartą el. paštu informavęs pareiškėją, kaip galima atpažinti sukčių ataką, t. y. kad pareiškėjas turi įvertinti, jog internetinis adresas turi būti *dnb.lt*, interneto svetainėse turi būti aktyvūs visi mygtukai, reikia patikrinti, ar atsidaręs tinklalapis atitinka realią banko interneto svetainę.

Lietuvos banko vertinimu, nagrinėjamu atveju bankas nepagrįstai perkelia visą atsakomybę pareiškėjui ir nurodo, kad pareiškėjas turi atlikti visus pirmiau minėtus veiksmus. Svarbu pažymėti, kad nagrinėjamo ginčo atveju matyti, kad suklastota svetainė tiek vizualiai (tiek pagal spalvą, tiek pagal išdėstytų mygtukų eilės tvarką), tiek dėl pateikiamos informacijos buvo itin panaši į tikrąją banko interneto svetainę. Vidutinis vartotojas, šiuo atveju ir pareiškėjas, siekdamas prisijungti prie internetinės banko paskyros, neprivalo tikrinti ir vertinti kiekvieno mygtuko funkcionalumo (paspausti ir patikrinti, ar visi mygtukai aktyvūs), žinoti, kokią informaciją, kokia tvarka ir išdėstymu įprastai bankas pateikia savo realioje interneto svetainėje, ir tikrinti ją kiekvieną kartą jungiantis prie banko interneto banko paskyros, ypač atsižvelgiant į tai, kad bankas bet kada tokią informaciją ir jos išdėstymą gali keisti.

Galiausiai, bankas savo klientus ragina nuolat tikrinti, ar interneto adresas atitinka realiai banko naudojamos svetainės adresą, kuriuo jungiamasi prie realios banko interneto banko aplinkos, t. y. *dnb.lt.* Lietuvos banko vertinimu, šie banko klientams pateikti įrodymai taip pat yra vertintini kritiškai, nes toks prisijungimo prie banko interneto banko paskyros adresas neatitinka realaus banko pavadinimo, todėl tiek pareiškėjas, tiek kiti klientai gali būti klaidinami, prie kurio banko paskyros jie jungiasi.

Atsižvelgiant į pirmiau išdėstytą informaciją, manytina, kad banko argumentai, kad pareiškėjas turėjo galimybę įvertinti atsiųstų tinklalapių nuorodų tikrumą ir jose teikiamą informaciją ir turėjo pastebėti, kad interneto svetainė yra suklastota, yra nepagrįsti, todėl atmestini.

Vis dėlto, išanalizavęs visas nustatytas aplinkybes ir ginčo byloje esančius duomenis, Lietuvos bankas daro išvadą, kad šiuo konkrečiu atveju vertinti pareiškėjo elgesio kaip atsargaus ir apdairaus ar tik neatsargaus nėra galima.

Kaip matyti iš nustatytų aplinkybių, Operaciją tretieji asmenys be pareiškėjo žinios galėjo atlikti tik dėl to, kad pareiškėjas, būdamas labai neatsargus, netinkamai įvykdė Mokėjimų įstatyme (34 straipsnis) ir su banku sudarytoje sutartyje įtvirtintus saugaus naudojimo reikalavimus. Remiantis nustatytais duomenimis, pareiškėjas, gavęs trečiųjų asmenų siųstą pranešimą, neįvertinęs, kad SMS pranešimas yra siunčiamas iš užsienyje registruoto telefono numerio ir parašytas be lietuviškų raidžių, nedvejodamas (kaip pripažįsta) paspaudė jame pateiktą nuorodą ir suklastotame interneto puslapyje nurodė savo personalizuotus saugumo duomenis, neįsitikinęs siųsto pranešimo ir jame pateiktos nuorodos tikrumu. Be to, pareiškėjas neįvertino jam „Smart-ID" programėlėje rodomos informacijos, kad jis ne tik jungiasi prie tariamai VMI aplinkos tam, kad susipažintų su administracinės nuobaudos pranešimu (būtent toks tikslas buvo nurodytas SMS pranešime), tačiau iškart (nesusipažinęs su jokiu pranešimu), „Smart-ID" programėlėje rodant tvirtinamą sumą, savo aktyviais veiksmais patvirtinto Operaciją.

Nurodytos aplinkybės leidžia teigti, kad pareiškėjas būtent dėl savo didelio neatsargumo neišsaugojo personalizuotų saugumo duomenų konfidencialumo – nesiėmė tų saugumo priemonių, kurių privalėjo imtis, kad būtų tinkamai apsaugoti jam suteiktos mokėjimo priemonės duomenys, ir pats patvirtino Operaciją.

---

[5] Paskelbtas tekstas: https://www.luminor.lt/lt/naujienos/luminor-perspeja-padaugejo-bandymu-isvilioti-pinigus

[6] https://www.vmi.lt/evmi/en/-/vmi-c4-afsp-c4-97ja-gyventojus-gavus-c4-aftartin-c4-85-prane-c5-a1im-c4-85-neskub-c4-97kite-atidaryti-nuorod-c5-b3

Konstatavus, kad pareiškėjas, nesilaikydamas jam, kaip mokėtojui, Mokėjimų įstatyme ir sutartyje su banku nustatytų pareigų, susijusių su išduotomis mokėjimo priemonėmis, elgėsi labai neatsargiai, kartu 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 šios priežasties, Lietuvos banko vertinimu, bankas neturi pareigos grąžinti (kompensuoti) pareiškėjui neautorizuotos Operacijos lėšų.

3. Dėl mokėjimo nurodymo neatšaukiamumo

Pareiškėjas kreipimesi, be kita ko, teigia, kad, supratęs, jog galėjo būti apgautas sukčių, iškart kreipėsi į banką telefonu, taip pat užpildė paraišką interneto banke atšaukti Operaciją, tačiau, nepaisydamas to, pareiškėjo teigimu, bankas Operaciją vis tiek įvykdė, lėšas pervesdamas gavėjo naudai. Pareiškėjas akcentavo ir tai, kad bankas iš karto neatsiliepė į pareiškėjo skambutį, o tai galėjo turėti įtakos Operacijos atšaukimo galimybei.

Vertinant pareiškėjo galimybę atšaukti jo vardu pateiktą mokėjimo nurodymą įvykdyti Operaciją, papildomai pažymėtina, kad, vadovaujantis Mokėjimų įstatymo 44 straipsnio 1 dalimi, mokėjimo paslaugų vartotojas negali atšaukti mokėjimo nurodymo po to, kai jį gauna mokėtojo mokėjimo paslaugų teikėjas, išskyrus šiame straipsnyje nustatytas išimtis. Minėto Mokėjimų įstatymo straipsnio 4 dalyje taip pat nustatyta, kad, pasibaigus 1 dalyje nurodytam laikotarpiui, mokėjimo nurodymas gali būti atšauktas tik tuo atveju, kai dėl to susitaria mokėjimo paslaugų vartotojas ir atitinkamas mokėjimo paslaugų teikėjas, o šio straipsnio 2 dalyje numatytais atvejais būtinas ir gavėjo sutikimas. Mokėjimo paslaugų teikėjas gali imti komisinį atlyginimą už mokėjimo nurodymo atšaukimą, jeigu tai numatyta bendrojoje sutartyje.

Taigi, pasibaigus Mokėjimų įstatymo 44 straipsnio 1 dalyje nurodytam terminui, mokėjimo nurodymas gali būti atšauktas tik dėl to susitarus vartotojui ir jo mokėjimo paslaugų teikėjui, todėl nurodytos galimybės (t. y. mokėjimo nurodymo atšaukimo) įtvirtinimas Mokėjimų įstatyme neturėtų būti vertinamas kaip priverstinis lėšų grąžinimas mokėtojui, esant jo atitinkamam prašymui (pasibaigus 44 straipsnio 1 dalyje nurodytam terminui).

Banko mokėjimo paslaugų teikimo sąlygų 6.3.3 papunktyje nurodyta, kad mokėjimo nurodymas negali būti atšauktas po to, kai jį iš mokėtojo gauna bankas, išskyrus šiose sąlygose nustatytais atvejais. Mokėjimo nurodymai, nustatyti sąlygų 6.4.2 papunktyje (t. y. kai susitariama juos įvykdyti konkrečią datą ar konkrečiu laikotarpiu), gali būti atšaukti ne vėliau kaip iki darbo dienos, einančios prieš sutartą dieną, pabaigos (6.3.5 papunktis). Pasibaigus banko mokėjimo paslaugų teikimo sąlygų 6.3.3 ir 6.3.5 papunkčiuose nustatytiems terminams, mokėjimo nurodymas gali būti atšauktas tik kliento ir banko susitarimu (6.3.6 papunktis).

Pažymėtina, kad nei Mokėjimų įstatyme, nei šalių susitarime (banko mokėjimo paslaugų teikimo sąlygose) nurodytos sąlygos atšaukti mokėjimo nurodymą įvykdyti Operaciją nagrinėjamo ginčo atveju nebuvo nustatytos, nes pareiškėjas į banką dėl Operacijos lėšų grąžinimo kreipėsi po to, kai sutikimas vykdyti minėtą mokėjimo operaciją jau buvo duotas ir banko mokėjimo paslaugų teikimo sąlygose nurodytas terminas atšaukti mokėjimo nurodymą jau buvo praėjęs[7].

Atkreiptinas dėmesys į tai, kad pareiškėjas kreipimesi į Lietuvos banką keletą kartų akcentavo, kad iš karto po Operacijos patvirtinimo skambino bankui, tačiau banko darbuotojai iš karto neatsiliepė, dėl to pareiškėjas galėjo patirti nuostolių.

Lietuvos banko vertinimu, remiantis bylos duomenimis ir pirmiau nurodytomis Mokėjimų įstatymo nuostatomis, objektyvaus ir pakankamo pagrindo teigti, kad užtrukęs banko specialistų atsiliepimas turėjo esminės reikšmės tam, kad Operacija būtų atšaukta, nėra. Iš banko pateiktų duomenų matyti, kad Operacija buvo įvykdyta kaip momentinis mokėjimas, t. y. nedelsiant, todėl jos atšaukti nebuvo galimybės net jeigu bankas būtų iš karto atsiliepęs į pareiškėjo skambutį. Dėl šios priežasties galima daryti išvadą, kad pareiškėjo argumentai, kad būtent dėl banko netinkamų veiksmų, t. y. pavėluoto atsiliepimo, Operacija negalėjo būti atšaukta, yra atmestini kaip nepagrįsti.

Pagal Mokėjimų įstatymo 46 straipsnį, mokėjimo paslaugų teikėjas privalo užtikrinti, kad po mokėjimo nurodymo gavimo mokėjimo operacijos suma būtų įskaityta į mokėjimo nurodyme nurodyto gavėjo sąskaitą minėtame straipsnyje nustatytais terminais, o Mokėjimų įstatymo 51 straipsnio 1 dalyje nustatyta mokėjimo paslaugų teikėjo atsakomybė už mokėtojo inicijuotos mokėjimo operacijos neįvykdymą, netinkamą ar pavėluotą įvykdymą. Aplinkybė, kad pareiškėjo

[7] Sutikimas Operacijai duotas 2023 m. balandžio 17 d. 16:04:16 val., o pareiškėjas į banką dėl Operacijos atšaukimo kreipėsi 2023 m. balandžio 17 d. 16:13:32 val. (paraiška interneto banke).

Operacija iš tiesų yra neautorizuota, nors ir atitiko pareiškėjo ir banko sutartą sutikimo atlikti mokėjimo operaciją davimo tvarką, paaiškėjo vėliau, nei ši Operacija buvo patvirtinta ir įvykdyta. Tai reiškia, kad šiuo atveju bankas neturėjo teisės aktuose nustatyto pagrindo tokio mokėjimo nurodymo nevykdyti ar jį atšaukti.

Įvertinus visa tai, kas išdėstyta pirmiau, ir nustačius, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, darytina išvada, kad pareiškėjo bankui keliamas reikalavimas grąžinti Operacijos sumą – 690 Eur, yra nepagrįstas, todėl atmestinas.

Remdamasis tuo, kas išdėstyta, ir vadovaudamasis Lietuvos Respublikos vartotojų teisių apsaugos įstatymo 27 straipsnio 1 dalies 3 punktu, Lietuvos banko valdybos 2012 m. sausio 26 d. nutarimo Nr. 03-23 „Dėl Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių patvirtinimo“ 2 punktu ir šiuo nutarimu patvirtintų Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių 59.3 papunkčiu, n u s p r e n d ž i u:

Atmesti pareiškėjo X. X. reikalavimą.

Lietuvos banko sprendimas dėl ginčo esmės yra rekomendacinio pobūdžio ir teismui neskundžiamas. Vartotojui ir finansų rinkos dalyviui išlieka teisė dėl ginčo sprendimo kreiptis į teismą 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