LIETUVOS BANKO PRIEŽIŪROS TARNYBOS FINANSINIŲ PASLAUGŲ IR RINKŲ PRIEŽIŪROS DEPARTAMENTO DIREKTORIUS

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

2020 m. sausio 15 d. Nr. 242-22
Vilnius

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

Nustatyta:

2019 m. rugsėjo 22 d. 12:17 val. pareiškėjas į savo telefono numerį gavo, kaip vėliau paaiškėjo, suklastotą ir į banko žinučių srautą įterptą SMS žinutę su pranešimu „Atnaujinkite „SmartID" paskyrą"[1]. Minėtoje žinutėje buvo pateikta aktyvi nuoroda. Pareiškėjas teigė, kad paspaudęs šią nuorodą pateko į, kaip vėliau paaiškėjo, suklastotą banko internetinės bankininkystės puslapį, vizualiai nesiskiriantį nuo įprasto puslapio. Suvedus banko ID ir asmens kodą buvo aktyvuota programėlė „SmartID" (toliau – „SmartID"). Pareiškėjas šioje programėlėje suvedė PIN1 ir PIN2 kodus, galvodamas, kad taip atnaujina „SmartID" paskyrą. Tačiau iš tikrųjų iš pareiškėjo banko sąskaitos 2019 m. rugsėjo 22 d. buvo nurašyta 1 499 Eur suma gavėjui *duomenys neskelbiami* – įvykdytas momentinis mokėjimas. Sukčiautojas bandė inicijuoti dar vieną mokėjimo pavedimą ir „SmartID" aktyvavosi dar kartą. Tik tada pareiškėjas suprato, kad buvo apgautas, o 1 499 Eur iš jo banko sąskaitos pasisavinti neteisėtu būdu. Pareiškėjas kreipėsi į banką dėl 1 499 Eur grąžinimo.

2019 m. rugsėjo 23 d. bankas pareiškėją informavo, kad kreipėsi į užsienio banką dėl 1 499 Eur grąžinimo ir gavo atsakymą, kad nėra galimybės grąžinti 1 499 Eur, nes lėšos iš sąskaitos paimtos. Bankas pareiškėjui papildomai nurodė, kad užsienio bankas prašo pateikti pareiškėjo kreipimosi į policiją kopiją.

2019 m. rugsėjo 23 d. pareiškėjas kreipėsi į Vilniaus apskrities vyriausiąjį policijos komisariatą prašydamas pradėti ikiteisminį tyrimą dėl neteisėtai iš pareiškėjo banko sąskaitos nuskaičiuotų 1 499 Eur.

2019 m. rugsėjo 25 d. pareiškėjas kreipėsi į Lietuvos banką dėl vartojimo ginčo nagrinėjimo ir prašė rekomenduoti bankui grąžinti neteisėtu būdu iš jo banko sąskaitos nurašytus 1 499 Eur. Kreipimesi pareiškėjas išdėstė pirmiau aprašytas aplinkybes, kaip buvo pateiktas vykdyti 1 499 Eur mokėjimo nurodymas, t. y. iš esmės pareiškėjas teigė neautorizavęs 1 499 Eur mokėjimo pavedimo gavėjui, o sukčiai neteisėtu būdu išviliojo PIN kodus ir taip iš jo banko sąskaitos pasisavino 1 499 Eur.

Bankas pateiktame atsiliepime Lietuvos bankui paaiškino, kad pareiškėjas, gavęs SMS žinutę, siųstą neva iš banko su *bit.ly* nuoroda į suklastotą e. banko sistemą, pats suvedė tik jam vienam žinomus „SmartID" PIN1 ir PIN2 kodus ir taip patvirtino mokėjimo nurodymą ir išreiškė sutikimą pervesti 1 499 Eur gavėjui *duomenys neskelbiami*.

Bankas paaiškino, kad mokėtojas sutikimą atlikti mokėjimo operaciją gali atšaukti iki mokėjimo nurodymo gavimo banke momento. Pareiškėjo atveju buvo inicijuotas ir patvirtintas momentinis mokėjimo nurodymas, kai lėšos nurašomos iš mokėtojo sąskaitos ir įskaitomos į gavėjo sąskaitą nedelsiant bet kuriuo paros metu, įskaitant ir savaitgalius bei švenčių dienas. Pareiškėjui kreipiantis į banką mokėjimo nurodymas jau buvo įvykdytas, lėšos buvo įskaitytos į gavėjo sąskaitą, todėl šiuo atveju mokėjimo nurodymas negalėjo būti

[1] „SmartID" – tai trečiosios šalies („SK ID Solutions AS") teikiama programėlė (aplikacija), atliekanti el. parašo ir el. atpažinties funkcijas. Lietuvoje veikiantys bankai šią programėlę laiko pagrindine priemone mokėjimo operacijoms autorizuoti, sutartims pasirašyti ar kitoms su banko veikla susijusioms operacijoms tvirtinti.

atšauktas.

Bankas teigė tarpininkavęs, kad pareiškėjui būtų sugrąžinti 1 499 Eur, ir kreipėsi į gavėjo banką dėl lėšų grąžinimo, tačiau iš gavėjo banko gavo atsakymą, kad lėšos iš gavėjo banko buvo išgrynintos.

Bankas atkreipė dėmesį, kad sukčiavimas, kai neva iš banko siunčiami SMS pranešimai su aktyvia (*bit.ly*) nuoroda į suklastotą e. banko sistemą, yra dar palyginti naujas sukčiavimo būdas Lietuvoje. Tokios SMS žinutės yra siunčiamos ne iš banko telefono numerio, sukčiai SMS žinutėms siųsti naudoja mobiliojo ryšio operatorių infrastruktūrą, mobilųjį ryšį ir standartinę SMS žinučių siuntimo paslaugos funkciją, kurią teikia mobiliojo ryšio operatoriai. Bankas teigė, kad, sulaukęs pirmų klientų pranešimų apie gautas neva iš banko SMS žinutes, ėmėsi priemonių: informacija apie naują sukčiavimo schemą ir pačios žinutės pavyzdys banko buvo paviešinti banko *Facebook* paskyroje, taip pat apie tai informuota žiniasklaida, o klientams išsiųsti el. laiškai. Toks laiškas pareiškėjui el. paštu buvo išsiųstas 2019 m. liepos 5 d. Bankas informaciją apie žinomus incidentus pateikė ir Lietuvos kriminaliniam policijos biurui bei Nacionaliniam kibernetiniam saugumo centrui.

Atsižvelgdamas į tai, kad mokėjimo nurodymas buvo patvirtintas PIN kodo slaptažodžiais ir nebuvo pagrindo mokėjimo nurodymo stabdyti arba atmesti, bankas prašė atmesti pareiškėjo reikalavimą kaip nepagrįstą.

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. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą ir jo pagrindu priimamas sprendimas.

Pareiškėjo ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjui 2019 m. rugsėjo 22 d. pareiškėjo banko sąskaitoje atliktos 1 499 Eur mokėjimo operacijos (toliau – ginčijama mokėjimo operacija) sumą. Pareiškėjas teigia, kad ginčijama mokėjimo operacija įvykdyta be pareiškėjo sutikimo, todėl bankas turi grąžinti pareiškėjui šios operacijos sumą. Bankas teigia, kad ginčijama mokėjimo operacija yra įvykdyta tinkamai, nes pareiškėjas savo sutikimą ją įvykdyti davė suvesdamas PIN1 ir PIN2 kodus (toliau – PIN kodai), todėl bankas neprivalo grąžinti pareiškėjui ginčijamos mokėjimo operacijos sumos.

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

Mokėjimo paslaugų teikėjų veiklą ir atsakomybę, mokėjimo paslaugas, jų teikimo sąlygas ir informavimo apie šias sąlygas reikalavimus, mokėjimo operacijų autorizavimą ir vykdymą, mokėjimo paslaugų vartotojų ir mokėjimo paslaugų teikėjų teises ir pareigas, susijusias su mokėjimo paslaugomis, kai mokėjimo paslaugų teikimas yra verslas, reglamentuoja Lietuvos Respublikos mokėjimų įstatymas (redakcija, galiojusi nuo 2019 m. gegužės 1 d. iki 2019 m. spalio 20 d.) (toliau – Mokėjimų įstatymas).

<u>Dėl ginčijamos mokėjimo operacijos autorizavimo</u>

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

Banko teigimu, pareiškėjo (mokėtojo) sutikimas įvykdyti ginčijamą mokėjimo operaciją buvo duotas vienu iš pareiškėjo ir banko sudarytoje bendrojoje sutartyje nurodytų būdų, t. y. pareiškėjui per mobilųjį telefoną prisijungus prie suklastotos interneto banko sistemos, joje

suvedus banko ID, asmens kodą, o „SmartID" programėlėje PIN kodus. Įvertinus pareiškėjo ir banko sudarytos bendrosios sutarties nuostatas, nustatyta, kad bendrąja sutartimi bankas ir pareiškėjas buvo susitarę, kad PIN kodo įvedimas laikomas pareiškėjo sutikimo atlikti mokėjimo operaciją davimu (bendrosios sutarties 11 skyrius „<...> *Parašas, įvestas PIN kodas arba aktyvintos bekontaktės mokėjimo kortelės prilietimas prie elektroninio kortelių skaitytuvo arba kitų pirmiau išvardintų, veiksmų rodo, kad sutinkate atlikti mokėjimo operaciją*"*).* Atsižvelgiant į tai, kad bendroji sutartis nustato banko ir pareiškėjo tarpusavio santykius, bei įvertinus tai, kad PIN kodas yra personalizuotas saugumo duomuo, kuris pripažįstamas neskelbtinu mokėjimo duomeniu (Mokėjimų įstatymo 2 straipsnio 41 dalis), darytina išvada, kad bendrojoje sutartyje nurodytas PIN kodo įvedimas pareiškėjo ir banko santykiuose laikytinas pareiškėjo sutikimu įvykdyti mokėjimo operaciją tik tada, kai tokį PIN kodą suveda pats pareiškėjas norėdamas pateikti vykdyti mokėjimo pavedimą.

Bankas pateikė jo vidaus sistemose užfiksuotus duomenis, pagrindžiančius, kad ginčijamos mokėjimo operacijos inicijavimo dieną prie interneto banko sistemos buvo jungtasi ir ginčijama mokėjimo operacija buvo patvirtinta panaudojant PIN kodus. Atkreiptinas dėmesys į tai, kad vien aplinkybė, jog mokėtojo mokėjimo paslaugų teikėjo vidaus sistemose užregistruotas mokėtojui išduotos mokėjimo priemonės, įskaitant jos personalizuotus saugumo duomenis (nagrinėjamu atveju – interneto banko ir PIN kodų), naudojimas, nelaikytina pakankamu įrodymu, kad mokėjimo priemone naudojosi ir (arba) mokėjimo operaciją autorizavo pats mokėtojas. 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).

Lietuvos bankas paprašė banko papildomai pateikti informaciją apie banko vidaus sistemose užfiksuotus įrenginių, kuriais šiam ginčui nagrinėti aktualiu laikotarpiu buvo jungtasi nuotoliniu būdu prie pareiškėjo interneto banko paskyros, IP adresus. Bankas pateikė banko vidaus sistemos išrašus, kuriuose pateikti duomenys apie laikotarpiu nuo 2019 m. rugsėjo 20 d. iki rugsėjo 23 d. banko sistemose fiksuotus IP adresus, kuriais buvo jungtasi prie pareiškėjo interneto banko paskyros (toliau – IP adresų sąrašas).

Iš Banko pateikto IP adresų sąrašo duomenų matyti, kad minimu laikotarpiu prie interneto banko buvo jungtasi iš šių IP adresų:

1) 2 dienos iki neautorizuotos mokėjimo operacijos atlikimo, t. y. 2019 m. rugsėjo 20 d., buvo jungtasi iš IP adreso Nr. *duomenys neskelbiami* (toliau – IP adresas Nr. 1);

2) 1 dieną iki neautorizuotos mokėjimo operacijos atlikimo, t. y. 2019 m. rugsėjo 21 d., prie interneto banko sistemos nebuvo iš viso jungtasi;

3) neautorizuotos mokėjimo operacijos atlikimo dieną, t. y. 2019 m. rugsėjo 22 d., buvo jungtasi iš IP adreso Nr. *duomenys neskelbiami* (toliau – IP adresas Nr. 2) ir IP adreso Nr. *duomenys neskelbiami* (toliau – IP adresas Nr. 3);

4) 1 dieną po neautorizuotos mokėjimo operacijos atlikimo, t. y. 2019 m. rugsėjo 23 d., buvo jungtasi iš IP adreso Nr. *duomenys neskelbiami* (toliau – IP adresas Nr. 4) ir IP adreso Nr. 1.

Lietuvos bankas paprašė pareiškėjo nurodyti įrenginių, kuriais pareiškėjas jungėsi nagrinėjamu laikotarpiu, IP adresus. Pareiškėjas nurodė IP adresus, kurie sutapo su banko pateiktame IP sąraše nurodytais IP adresais Nr. 1 ir Nr. 3.

Kaip minėta prieš tai, remiantis pareiškėjo nurodyta informacija, pareiškėjas 2019 m. rugsėjo 22 d. 12:17 val. į savo mobiliųjį telefoną gavo į banko žinučių srautą įterptą SMS žinutę, kurioje buvo prašoma atnaujinti „SmartID" paskyrą, ir pagal žinutėje pateiktą nuorodą prisijungė prie interneto banko paskyros, kuri, kaip vėliau paaiškėjo, buvo suklastota (toliau – suklastota interneto banko paskyra). Pareiškėjas teigia prie suklastotos interneto banko paskyros prisijungęs iš karto, kai tik gavo minėtą SMS žinutę, tikėdamasis, kad vykdo banko nurodymus atnaujinti „SmartID" paskyrą, kaip tai buvo nurodyta pareiškėjo gautoje SMS žinutėje, ir suklastotoje interneto banko paskyroje suvedė savo asmens kodą ir banko ID, o „SmartID" programėlėje PIN kodus, turėdamas tikslą atnaujinti „SmartID".

Tai, kad pareiškėjas prisijungė prie suklastotos interneto banko paskyros, liudija ir banko Lietuvos bankui pateikto IP adresų sąrašo duomenys. IP adresų sąraše duomenų apie tai, kad pareiškėjas 2019 m. rugsėjo 22 d. apie 12 val. 17 min. būtų jungęsis prie interneto banko sistemos, nėra. Atkreiptinas dėmesys į tai, kad IP adresų sąraše pirmasis 2019 m. rugsėjo 22 d. jungimasis prie interneto banko užfiksuotas 12 val. 36 min., t. y. praėjus apie 19 minučių po galimo pareiškėjo jungimosi prie suklastotos interneto banko

paskyros. Banko pateikto IP adresų sąrašo duomenimis, prie interneto banko tuo metu buvo jungtasi iš IP adreso Nr. 2. Būtent iš IP adreso Nr. 2 buvo inicijuota ir ginčijama mokėjimo operacija. Kompleksiškai vertinant pareiškėjo ir banko pateiktą informaciją, darytina išvada, kad 2019 m. rugsėjo 22 d. 12 val. 36 min. prie interneto banko jungėsi ne pats pareiškėjas, o tretieji asmenys, kurie, nukreipdami pareiškėją į suklastotą banko interneto banko paskyrą, neteisėtai išviliojo ir pasisavino prisijungti prie interneto banko sistemos reikalingus duomenis ir juos panaudojo tos pačios dienos 12 val. 36 min. iš IP adreso Nr. 2 prisijungdami prie pareiškėjo interneto banko paskyros ir joje inicijuodami dvi mokėjimo operacijas.

Pareiškėjas Lietuvos bankui taip pat nurodė, kad, suvedus į suklastotą interneto banko paskyrą banko ID, asmens kodą, o SmartID programėlėje PIN kodus, sistema jo paprašė įvesti PIN kodus pakartotinai. Ši aplinkybė sukėlė pareiškėjui įtarimų, todėl suklastotoje interneto paskyroje prašomų duomenų pareiškėjas pakartotinai nebepateikė. Analizuojant IP adresų sąrašo duomenis, matyti, kad iš IP adreso Nr. 2 prie interneto banko neteisėtai prisijungę asmenys inicijavo dvi mokėjimo operacijas, iš kurių viena buvo įvykdyta (ginčijama mokėjimo operacija), o kita – ne. Kompleksiškai vertinant pareiškėjo nurodytas aplinkybes ir IP adresų sąrašo duomenis, darytina išvada, kad viena iš inicijuotų mokėjimo operacijų (paskesnė) buvo neįvykdyta tik dėl to, kad pareiškėjas suklastotoje interneto banko paskyroje pakartotinai nebesuvedė PIN2 kodo, kuris būtinas mokėjimo operacijai patvirtinti, t. y. dėl to, kad tretiesiems asmenims apgaulės būdu nepavyko išvilioti iš pareiškėjo šio kodo ir jį panaudoti tikrojoje banko interneto sistemoje šių trečiųjų asmenų inicijuotai mokėjimo operacijai patvirtinti. Kita vertus, pirmoji trečiųjų asmenų inicijuota mokėjimo operacija (ginčijama mokėjimo operacija) buvo patvirtinta, šiems tretiesiems asmenims panaudojus nusavintus pareiškėjo banko ID, asmens kodą, kuriuos pareiškėjas suvedė į suklastotą interneto banko paskyrą pirmąjį kartą bei „SmartID" programėlėje PIN kodus, manydamas, kad tą daro „SmartID" paskyros atnaujinimo tikslais, bet ne siekdamas patvirtinti 1 499 Eur mokėjimo nurodymą.

Pareiškėjas teigia, kad dėl daugkartinio „SmartID" duomenų prašymo jam kilo įtarimų, todėl tą pačią dieną, t. y. 2019 m. rugsėjo 22 d., 12 val. 45 min. pareiškėjas prisijungė prie interneto banko ne per SMS žinutėje pateiktą nuorodą ir pastebėjo, kad iš jo banko sąskaitos buvo atlikta ginčijama mokėjimo operacija. Šios pareiškėjo nurodytos aplinkybės sutampa ir su IP adresų sąraše nurodytais duomenimis, t. y. IP adresų sąraše 2019 m. rugsėjo 22 d. 12 val. 45 min. yra užfiksuotas jungimasis prie interneto banko iš IP adreso Nr. 3. Kaip minėta prieš tai, pareiškėjas patvirtino, kad IP adresas Nr. 3 priklauso pačiam pareiškėjui.

Būtina pažymėti, kad bankas neginčijo pareiškėjo nurodytų aplinkybių, kad atidaręs SMS žinute jam siųstą aktyvią nuorodą pareiškėjas pateko į sukčių suklastotą interneto banko paskyrą, joje suvedė savo banko ID, asmens kodą, o „SmartID" programėlėje PIN kodus ir dėl to buvo įvykdytas 1 499 Eur mokėjimas.

Be kita ko, bankas savo paaiškinimuose nurodė ir tai, kad apie tokius sukčiavimo būdus bankui jau buvo žinoma anksčiau.

Įvertinus pareiškėjo ir banko pateiktą informaciją apie faktines ginčijamos mokėjimo operacijos inicijavimo ir atlikimo aplinkybes, darytina išvada, kad ginčijamą mokėjimo operaciją banko interneto banko sistemoje inicijavo ir sutikimą jai įvykdyti davė ne pats pareiškėjas, o tretieji asmenys, todėl pagrindo teigti, kad pareiškėjas davė sutikimą atlikti ginčijamą mokėjimo operaciją, kaip toks susitikimas suprantamas Mokėjimų įstatymo 29 straipsnio 1 dalies kontekste, nėra, t. y., Lietuvos banko vertinimu, ginčijama mokėjimo operacija laikytina neautorizuota.

<u>Dėl neautorizuotos mokėjimo operacijos pasekmių ir pareiškėjo teisės į ginčijamos mokėjimo operacijos sumos grąžinimą</u>

Mokėjimų įstatymo 36 straipsnio 1 dalyje nustatyta mokėtojo mokėjimo paslaugų teikėjo pareiga grąžinti mokėtojui neautorizuotos mokėjimo operacijos sumą, jeigu mokėtojas, sužinojęs apie neautorizuotas operacijas, apie tai praneša savo mokėjimo paslaugų teikėjui nedelsdamas, ne vėliau kaip per 13 mėnesių nuo lėšų nurašymo datos. Vadovaujantis Mokėjimų įstatymo 38 straipsnio 1 dalimi, neautorizuota mokėjimo operacija turi būti grąžinta mokėtojui nedelsiant, bet ne vėliau kaip iki kitos darbo dienos pabaigos, po to, kai mokėjimo paslaugų teikėjas sužino apie neautorizuotą mokėjimo operaciją.

Pažymėtina, kad mokėtojo mokėjimo paslaugų teikėjas gali būti visiškai atleistas nuo pareigos grąžinti mokėtojui mokėjimo operacijos sumą tik tuo atveju, jeigu įrodomas mokėtojo sukčiavimas (nesąžiningumas arba tyčia) arba didelis neatsargumas (Mokėjimų

įstatymo 37 straipsnio 3 dalis ir 39 straipsnio 3 dalis).

Remiantis pareiškėjo ir banko pateikta informacija, apie tai, kad pareiškėjas neigia autorizavęs ginčijamą mokėjimo operaciją, bankas buvo informuotas tą pačią dieną, kai tik buvo įvykdyta ginčijama mokėjimo operacija, t. y. 2019 m. rugsėjo 22 d. (pareiškėjas nurodė, kad telefonu banką informavo nedelsdamas ir tą pačią dieną apie 15 val. atvyko į banko padalinį). Pareiškėjas tvirtina, kad, pastebėjęs, jog iš jo banko sąskaitos buvo nurašytos piniginės lėšos, skirtos ginčijamai mokėjimo operacijai įvykdyti, nedelsdamas kreipėsi į banką ir pranešė jam apie tai, kad ginčijama mokėjimo operacija yra neautorizuota, taip pat paprašė banko sustabdyti tokios mokėjimo operacijos vykdymą. Tačiau bankas pareiškėjui nurodė neturintis galimybės atšaukti ginčijamos mokėjimo operacijos, nes buvo atliktas momentinis mokėjimas, taigi, pareiškėjui kreipusis į banką dėl ginčijamos mokėjimo operacijos atšaukimo, mokėjimo operacija jau buvo įvykdyta, t. y. mokėjimo nurodyme nurodytas lėšų gavėjas jau buvo gavęs ginčijamos mokėjimo operacijos sumą.

Nepaisant to, kad bankas galimybės atšaukti įvykdytą ginčijamą mokėjimo operaciją nebeturėjo, apie tai, kad pareiškėjas neigia autorizavęs ginčijamą mokėjimo operaciją, bankui tapo žinoma nuo pareiškėjo kreipimosi į banką dienos.

Mokėjimų įstatymo 39 straipsnio 2 dalyje nustatyta, kad 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); nuostoliai yra patirti dėl mokėjimo paslaugų teikėjo, jo darbuotojo, tarpininko, filialo ar asmenų, kuriems perduotas veiklos funkcijų valdymas, veiksmų ar neveikimo (2 punktas).

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.

Nagrinėjamo ginčo byloje buvo nustatyta, kad tretieji asmenys, pareiškėjui to nežinant ir nesuprantant, neteisėtai išviliojo iš pareiškėjo mokėjimo priemonės, t. y. interneto banko personalizuotus saugumo duomenis ir juos panaudojo neteisėtai prisijungti prie interneto banko ir ginčijamai mokėjimo operacijai inicijuoti. Įvertinus pareiškėjo ir banko pateiktą informaciją apie trečiųjų asmenų neteisėtus veiksmus, dėl kurių iš pareiškėjo banko sąskaitos, nesant pareiškėjo sutikimo, buvo įvykdyta ginčijama mokėjimo operacija, galima pagrįstai daryti išvadą, kad atliekant ginčijamą mokėjimo operaciją banko pareiškėjui išduota mokėjimo priemonė, t. y. interneto bankas, įskaitant jos personalizuotus saugumo duomenis, buvo neteisėtai pasisavinta. Vertinant, ar pareiškėjas galėjo pastebėti mokėjimo priemonės praradimą iki ginčijamos mokėjimo operacijos įvykdymo, būtina atsižvelgti į tai, kad: 1) pareiškėjas SMS žinutę, kurioje pareiškėjo buvo prašoma atnaujinti „SmartID“ paskyrą, gavo neva iš paties banko, įterptą į kitų prieš tai pareiškėjui siųstų banko žinučių srautą; 2) atidaręs aktyvią nuorodą, pareiškėjas pateko į suklastotą interneto banko paskyrą, kuri jam objektyviai galėjo atrodyti kaip tikra interneto banko aplinka; 3) personalizuotus saugumo duomenis pareiškėjas atskleidė norėdamas atnaujinti „SmartID“ programėlę, o ne siekdamas įvykdyti ginčijamą arba bet kurią kitą mokėjimo operaciją; 4) apie tai, kad suklastotoje interneto banko paskyroje įvesti personalizuoti saugumo duomenys tapo žinomi tretiesiems asmenims ir šie asmenys juos panaudojo ginčijamai mokėjimo operacijai atlikti, pareiškėjui, turimais ginčo bylos duomenimis, tuo metu nebuvo žinoma; 5) apie šias aplinkybes pareiškėjas sužinojo tik po to, kai gavo įtarimą sukėlusį prašymą suklastotoje interneto banko paskyroje pakartotinai suvesti PIN kodus ir prie tikrosios interneto banko paskyros prisijungė per oficialią banko interneto svetainę, o ne per telefonu SMS žinutėje pateiktą nuorodą; 6) sužinojęs, kad yra atlikta ginčijama mokėjimo operacija ir pasisavinti personalizuoti saugumo duomenys bei interneto bankas, pareiškėjas nedelsdamas kreipėsi į banką ir informavo jį apie tai, kad ginčijama mokėjimo operacija yra neautorizuota. Šalių ginčo dėl to, kad pareiškėjas galėjo veikti nesąžiningai arba tyčia, įskaitant sukčiavimą, nėra, todėl darytina išvada, kad bankas pripažįsta, kad pareiškėjo veiksmuose neįžvelgia nesąžiningumo ir (arba) tyčios, t. y. neįžvelgia pareiškėjo veiksmuose galimo sukčiavimo požymių. Lietuvos banko vertinimu, visos šios aplinkybės rodo, kad pareiškėjas tenkina Mokėjimų įstatymo 39 straipsnio 2 dalies 1 punkte nurodytas sąlygas, atleidžiančias mokėtoją nuo bet kokių nuostolių, susijusių su neautorizuotos mokėjimo operacijos atlikimu, t. y. pareiškėjo ir banko pateikta informacija

nesudaro pagrindo teigti, kad iki ginčijamos mokėjimo operacijos įvykdymo pareiškėjas galėjo žinoti arba pastebėti, kad mokėjimo priemonė (interneto bankas), įskaitant personalizuotus saugumo duomenis, buvo neteisėtai pasisavinta.

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 arba dėl didelio neatsargumo neįvykdęs vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų. Tokiais atvejais šio straipsnio 1 dalyje nustatytas didžiausios nuostolių sumos ribojimas netaikomas.

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).

Siekiant įvertinti, ar ginčo byloje pareiškėjo atžvilgiu galėtų būti taikoma Mokėjimo įstatymo 39 straipsnio 3 dalis, būtina nustatyti, ar pareiškėjo elgesys, atidarant SMS žinute gautą nuorodą ir suklastotoje banko interneto paskyroje suvedant personalizuotus saugumo duomenis, o „SmartID" programėlėje – PIN kodus, gali būti vertinamas kaip didelis pareiškėjo neatsargumas (aplaidumas), dėl kurio visi nuostoliai, susiję su ginčijamos mokėjimo operacijos įvykdymu, turėtų tekti pareiškėjui. Kaip ir minėta prieš tai, paties pareiškėjo sukčiavimo (nesąžiningumas arba tyčia) aplinkybė nėra vertinama, nes ginčo byloje duomenų apie galimą pareiškėjo sukčiavimą nėra, o ginčo šalys galimo sukčiavimo aplinkybe nesiremia.

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

Kasacinis teismas civilinėje byloje (byla Nr. 3K-3-222-219/2017) pateikė išaiškinimą, kas galėtų būti laikoma dideliu neatsargumu teikiant mokėjimo paslaugas: „Teisėjų kolegija nurodo, kad ieškovas suprato arba turėjo suprasti, kad jam atsakovės suteikti slapti ir tik jam žinomi prisijungimo prie sąskaitų duomenys apsaugo jo sąskaitas. Jų atskleidimas tretiesiems asmenims, juo labiau neidentifikuotiems telefoniniu ryšiu, pažeidė sąskaitų apsaugą ir sudarė galimybę tretiesiems asmenims pasinaudoti sąskaitose esančiais pinigais, todėl personalizuotų (slaptų, žinomų tik vartotojui) prisijungimo prie sąskaitų duomenų atskleidimas telefoniniu ryšiu tretiesiems asmenims rodo ne tik ieškovo neteisėtus, pažeidžiančius sutarties sąlygas veiksmus (Mokėjimų įstatymo 25 straipsnis), bet ir neprotingą, išskirtinai nerūpestingą elgesį, kuris kvalifikuotinas kaip didelis neatsargumas, lėmęs pinigų iš jo sąskaitų pervedimą tretiesiems asmenims. Todėl jam tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai (Mokėjimų įstatymo 30 straipsnio 2 dalis)."

Bankas, siekdamas pagrįsti, kad pareiškėjas, atidarydamas SMS žinute gautą nuorodą ir suklastotoje interneto banko paskyroje suvesdamas banko ID, savo asmens kodą, o „SmartID" programėlėje PIN1 bei PIN2, nebuvo pakankamai rūpestingas ir apdairus, remiasi aplinkybe, kad dar 2019 m. liepos 5 d. pareiškėjui elektroniniu paštu buvo siųstas informacinis pranešimas, įspėjantis apie sukčių platinamas neva banko siunčiamas SMS žinutes. Banko Lietuvos bankui pateikto pareiškėjui siųsto pranešimo tekste nurodoma tai: „Norime įspėti, kad pastaruoju metu padažnėjo pranešimų apie SMS žinutes, neva siunčiamas iš SEB banko. Žinutės gavėjus sukčiai informuoja apie gautą pranešimą, kuris yra atsiųstoje nuorodoje į netikrą interneto banko svetainę. Spustelėjęs nuorodą žinutės gavėjas yra prašomas įvesti savo interneto banko atpažinimo ir asmens kodus, telefono numerį, patvirtinti PIN kodus. Taip sukčiai bando išvilioti prisijungimo prie interneto banko duomenis ir pasisavinti svetimas lėšas." Minėtame pranešime bankas taip pat atkreipė dėmesį, kad bankas nesiunčia SMS žinučių, kuriose yra aktyvios nuorodos į interneto banką, jungiantis prie interneto banko geriau patiems vartotojams įvesti banko interneto adresą, PIN kodus vesti tik tada, kai pats mokėtojas atlieka mokėjimo operacijas. Bankas taip pat pranešime pateikė vaizdinę informaciją, kaip galėtų atrodyti sukčių siunčiama žinutė. Pareiškėjas neneigė gavęs tokią žinutę iš banko.

Vis dėl to, Lietuvos banko nuomone, nepaisant to, kad pareiškėjas buvo informuotas apie panašius galimus sukčiavimo būdus, vien ši aplinkybė nelaikytina pakankamu pagrindu

pareiškėjo elgesį vertinti kaip didelį neatsargumą. Didelis neatsargumas turėtų būti objektyviai aiškus, t. y. pasireikšti esminiu pareigos elgtis rūpestingai pažeidimu ir (arba) atsargumo priemonių nepaisymu, asmens galėjimu numatyti tokio nerūpestingo elgesio pasekmes bei veiksmų išvengti tokių pasekmių nesiėmimu. Antrosios mokėjimo paslaugų direktyvos (toliau – PSD2) preambulės 72 punkte rašoma, kad „siekiant įvertinti galimą mokėjimo paslaugų vartotojo aplaidumą ar didelį aplaidumą, reikėtų atsižvelgti į visas aplinkybes. Įtariamo aplaidumo įrodymai ir laipsnis paprastai turėtų būti vertinami pagal nacionalinę teisę. Tačiau nors aplaidumo sąvoka reiškia, kad pažeidžiamas įsipareigojimas elgtis rūpestingai, didelis aplaidumas turėtų reikšti daugiau nei vien aplaidumą ir apimti labai nerūpestingą elgesį; pavyzdžiui, tai būtų mokėjimo operacijos autorizavimui naudojamų saugumo požymių laikymas prie mokėjimo priemonės atviru ir trečiosioms šalims lengvai atskleidžiamu formatu."

Lietuvos banko vertinimu, šio konkretaus ginčo aplinkybių visuma nesudaro pagrindo manyti, kad pareiškėjo veiksmai galėtų turėti didelio neatsargumo (aplaidumo) požymių.

Pirma, pareiškėjas į savo telefono numerį gavo suklastotą SMS žinutę, kuri buvo įterpta į tikrų prieš tai pareiškėjo iš banko gautų žinučių srautą. Kadangi gauta žinutė buvo įterpta į kitų banko siųstų SMS žinučių srautą, pareiškėjui objektyviai galėjo atrodyti, kad ją siuntė bankas, todėl vien ši aplinkybė galėjo sumažinti pareiškėjo budrumą. Normalu, kad pareiškėjas, būdamas vidutinis vartotojas, iš karto negalėjo suprasti, kad žinutę siuntė ne bankas.

Taip pat papildomai svarbu atkreipti dėmesį, kad banko Bendrųjų mokėjimo paslaugų taisyklių 9 skyriuje nurodoma, kad „<...>Bendrąją sutartį mes galime nutraukti prieš tai jūsų neinformavę tik esant tokioms svarbioms priežastims kaip šios: pateikėte neteisingą, ne visą informaciją, atsisakote ją pateikti arba *atnaujinti* (jeigu mums ši informacija yra esminė)<...>" Pareiškėjas pagrįstai galėjo tikėtis, kad tinkamai vadovaujasi banko Bendrųjų mokėjimo paslaugų taisyklėmis ir atlieka tuos veiksmus, kurių reikalauja bankas, t. y. atnaujina „SmartID" programėlę. Atsižvelgiant į tai, kad sukčių siųsta SMS žinutė buvo įterpta į tikrų banko žinučių srautą, į tai, kad buvo suklastota elektroninė banko aplinka, galima teigti, kad pareiškėjas negalėjo suprasti, kad jo veiksmai yra ne banko pateiktų nurodymų vykdymas, o sukčių ataka.

Antra, Lietuvos banko vertinimu, negalima teigti, kad pareiškėjo elgesys (atidarė gautoje SMS žinutėje pateiktą nuorodą ir suvedė banko ID ir savo asmens kodą, o „SmartID" paskyroje – PIN1 bei PIN2, vykdydamas suklastotoje interneto banko paskyroje pateiktus nurodymus) gali būti vertinamas kaip itin nerūpestingas (aplaidus) elgesys. Kaip jau buvo minėta, pareiškėjas tretiesiems asmenims nepadiktavo PIN kodų slaptažodžių ar kitaip itin nerūpestingai nesielgė, kad šie PIN kodai galėtų tapti žinomi tretiesiems asmenims, o tik vykdė sukčių atsiųstoje SMS žinutėje, įterptoje tarp kitų tikrų banko žinučių, esančioje nuorodoje pateiktus nurodymus, manydamas, kad atnaujina „SmartID" programėlę, suvedė PIN kodo slaptažodžius, kuriais buvo patvirtintas sukčių suformuotas 1 499 Eur mokėjimo nurodymas. Pažymėtina, kad, pagal viešai prieinamas „SmartID" naudojimo sąlygas vertinant aplinkybę, kad PIN2 kodo slaptažodis yra naudojamas ne tik mokėjimo operacijai patvirtinti bet ir susitarimams patvirtinti, pareiškėjui objektyviai galėjo atrodyti, kad „SmartID" paskyros atnaujinimas suvedant PIN2 kodą yra normalus veiksmas, kuriuo patvirtinamas sutikimas atnaujinti programėlę. Be to, iš banko Lietuvos bankui pateiktos informacijos apie tai, kaip pareiškėjas naudojo „SmartID" paskyrą, matyti, kad pareiškėjas prieš tai nebuvo atlikęs „SmartID" atnaujinimo. Viešai prieinamose „SmartID" naudojimo sąlygose[2] vartotojams pateikiama informacija apie „SmartID" programėlės atnaujinimą: „reguliarus „SmartID" programėlės naujinimas padeda užtikrinti, kad jūsų duomenys bus saugūs, o programėlė sklandžiai veiks. Nuo 2019 m. liepos mėn. „SmartID" blokuos naudojimąsi pasenusiomis programėlėmis. Tokiu atveju bus rodomas klaidos pranešimas, kuriame paaiškinama problema, kylanti kiekvieną kartą bandant naudoti „SmartID". Norėdami ją išspręsti, atsisiųskite ir įdiekite naujausią programėlės versiją, kurią visada galima nemokamai atsisiųsti „Google Play" ir „AppStore" parduotuvėse." Taigi, įvertinus faktą, kad SMS žinutė su prašymu atnaujinti „SmartID" programėlę pareiškėjui buvo atsiųsta tarp kitų tikrų banko žinučių, taip pat atsižvelgiant į „SmartID" naudojimo sąlygose pateikiamą informaciją apie „SmartID" programėlės atnaujinimą (PIN naudojamas susitarimams patvirtinti ir pateikiama informacija

[2] https://www.smart-id.com/lt/pagalba/duk/perspejimai-ir-apribojimai/reikalingas-ismaniojo-identifikavimo-atnaujinimas/

apie būtinybę atnaujinti „SmartID“), darytina išvada, kad pareiškėjas galėjo pagrįstai tikėtis, kad, vesdamas banko ID, asmens kodą bei „SmartID“ programėlėje PIN kodus, jis elgiasi rūpestingai ir atnaujina savo „SmartID“.

Trečia, pažymėtina, kad pats bankas aktyviai savo klientams siūlo naudotis „SmartID“ programėle, savo interneto svetainėje pateikia informaciją apie naudojimąsi programėle, todėl banko paslaugų vartotojams, įskaitant ir pareiškėją, pagrįstai gali nekilti abejonių, kad bankas prašo atlikti veiksmus, susijusius su „SmartID“ (šiuo atveju atnaujinti programėlę).

Be to, atkreiptinas dėmesys į tai, kad netgi ir pats bankas savo 2019 m. rugsėjo 26 d. atsakyme pareiškėjui pripažino, kad sukčių ataka buvo parengta itin gerai, toks sukčiavimo būdas yra naujas Lietuvoje, todėl suklastota SMS žinutė, gauta kitų tikrų banko žinučių sraute, galėjo sukelti pareiškėjo pasitikėjimą ir jį suklaidinti.

Taigi, atsižvelgiant į visų ginčo byloje nustatytų aplinkybių kontekstą, pareiškėjo elgesys atidarant sukčių SMS žinute gautą nuorodą ir suvedant PIN1 bei PIN2 kodus negalėtų būti laikomas dideliu neatsargumu. Kaip minėta, tiek Kasacinio teismo praktikoje, tiek PSD2 aiškiai pasisakoma, kad didelis neatsargumas turėtų pasireikšti labai dideliu aplaidumu. Nagrinėjamo ginčo atveju iš konkrečių tik šioje ginčo byloje nustatytų aplinkybių matyti, kad pareiškėjas nesielgė itin nerūpestingai (aplaidžiai), o dėl gerai parengtos sukčių atakos suklastotoje interneto banko paskyroje suvedė banko ID, asmens kodą, o „SmartID“ programėlėje PIN1 ir PIN2 kodus, dėl to buvo pateiktas vykdyti 1 499 Eur momentinis mokėjimas.

Pažymėtina, kad aplinkybės, jog pareiškėjas kilus įtarimų dėl galimo sukčiavimo iš karto patikrino savo banko sąskaitą, kreipėsi į banką ir banką informavo apie neautorizuotą mokėjimo operaciją, rodo, kad pareiškėjas elgėsi rūpestingai ir vykdė savo pareigą pranešti bankui apie mokėjimo priemonės neteisėtą pasisavinimą.

Įvertinus pirmiau išdėstytą informaciją, konstatuotina, kad pagrindo pareiškėjo atžvilgiu taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį nėra. Kitų aplinkybių, kurios leistų pagrįstai manyti, kad pareiškėjui turėtų tekti visi su ginčijama mokėjimo operacija susiję nuostoliai, ginčo byloje tai pat nenustatyta, todėl, Lietuvos banko vertinimu, pareiškėjas turi teisę susigrąžinti ginčijamos mokėjimo operacijos, kuri buvo neautorizuota, lėšas (1 499 Eur).

<u>Dėl banko sprendimo atsisakyti grąžinti ginčijamos mokėjimo operacijos sumą pagrįstumo</u>

Atsižvelgiant į tai, kad šioje ginčo byloje iš nustatytų aplinkybių visumos konstatuotina, kad banko iš pareiškėjo banko sąskaitos įvykdyta 1 499 Eur mokėjimo operacija gavėjui laikytina pareiškėjo neautorizuota, nes inicijuojant mokėjimo operaciją banko veiklą paveikė sukčių ataka, pareiškėjo mokėjimo priemonė buvo neteisėtai pasisavinta, banko pateikti įrodymai ginčo byloje nepatvirtina pareiškėjo didelio neatsargumo ar sukčiavimo fakto, ir vadovaujantis Mokėjimų įstatymo 39 straipsnio 2 dalies bei 38 straipsnio 1 dalies nuostatomis, darytina išvada, kad ginčo byloje nėra nustatyta pagrindų atleisti banką nuo pareigos grąžinti pareikėjo neautorizuotos 1 499 Eur mokėjimo operacijos sumą, todėl banko atsisakymas grąžinti 1 499 Eur mokėjimo operacijos sumą yra nepagrįstas.

Apibendrinus pirmiau išdėstytą informaciją, darytina išvada, kad bankas turi pareiškėjui grąžinti visą 1 499 Eur neautorizuotos mokėjimo operacijos sumą, įskaitant ir komisinį mokestį už mokėjimo pavedimo atlikimą.

Papildomai pažymėtina, kad nagrinėjamo ginčo byloje pareiškėjas nenurodė, kad dėl neautorizuotos 1 499 Eur mokėjimo operacijos patyrė kitų nuostolių, ir bankui nekėlė reikalavimo juos atlyginti, todėl sprendime šis aspektas nėra analizuojamas.

Remdamasis tuo, kas išdėstyta, ir vadovaudamasis Vartotojų teisių apsaugos įstatymo 27 straipsnio 1 dalies 1 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 59.1 papunkčiu, n u s p r e n d ž i u:

1. Tenkinti pareiškėjo X.X. reikalavimą ir rekomenduoti bankui grąžinti pareiškėjui 1 499 Eur.

2. Įpareigoti banką per mėnesį nuo šio sprendimo priėmimo dienos raštu informuoti Lietuvos banką apie šio sprendimo rezoliucinės dalies 1 punkte nurodytos rekomendacijos įgyvendinimą (neįgyvendinimą). Bankui neįvykdžius minėtos rekomendacijos, tai bus

paskelbta Lietuvos Respublikos teisės aktų nustatyta tvarka.

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.

Reguliuojamos rinkos priežiūros skyriaus
viršininkas, pavaduojantis Finansinių paslaugų
ir rinkų priežiūros departamento direktorių Vaidas Cibas