LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

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

[Data] Nr. [Nr.]
Vilnius

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

N u s t a t y t a:

2021 m. spalio 19 d. nuo 19 val. 38 min. iki 19 val. 46 min. iš pareiškėjo sąskaitų Nr. LT *duomenys neskelbiami* ir LT *duomenys neskelbiami* banke buvo inicijuotos dvi po 3 800 Eur mokėjimo operacijos, kurių bendra suma – 7 600 Eur (toliau – mokėjimo operacijos), lėšas pervedant lėšų gavėjui Yoh'ui Coulibaly (Yoh Coulibaly) (toliau – gavėjas).

19 val. 44 min. pareiškėjas telefonu kreipėsi į banką ir informavo, kad iš banko gavo SMS žinutę, kad jo vardu yra sukurta nauja „Smart-ID" paskyra ir kad jeigu pareiškėjas šio veiksmo neatliko, turėtų skubiai susisiekti su banku. Pareiškėjas banko darbuotojui telefonu paaiškino, kad prieš tai savo telefono numeriu gavo SMS žinutę, kurioje buvo pranešama, kad pareiškėjo paskyroje yra aptikta įtartina veikla, ir jo buvo prašoma paspausti SMS žinutėje pateiktą aktyvią nuorodą. Paspaudęs šią nuorodą pareiškėjas pateko į interneto puslapį, vizualiai panašų į banko interneto puslapį, ir jame suvedė savo personalizuotus saugos duomenis (asmens kodą, banko atpažinimo kodą) bei savo mobiliajame įrenginyje suvedė „Smart-ID" PIN1 ir PIN2 kodus. Pareiškėjas taip pat teigė, kad SMS žinutė buvo įsiterpusi į tikrų banko žinučių srautą, todėl pareiškėjas manė, kad vykdo banko jam pateiktus nurodymus.

Atlikęs tyrimą bankas nustatė, kad 2021 m. spalio 19 d. 19 val. 20 min. pareiškėjas į savo mobilųjį telefoną Nr. *duomenys neskelbiami* iš trečiųjų asmenų gavo SMS žinutę su tokiu tekstu: *„Jusu paskyroje aptikta itartinos veiklos, spustelekite sia nuoroda, kad to isvengtume: HK32937.com.*" Pareiškėjas paspaudė pateiktą aktyvią nuorodą ir pateko į trečiųjų asmenų suklastotą banko interneto banko puslapį, jame suvedė savo banko atpažinimo kodą, asmens kodą, taip pat savo mobiliajame įrenginyje į savo „Smart-ID" paskyrą suvedė „Smart-ID" PIN1 ir PIN2 kodus. Tokie pareiškėjo veiksmai lėmė tai, kad tretieji asmenys pasisavino pareiškėjo personalizuotus saugos duomenis ir 2021 m. spalio 19 d. 19 val. 26 min. savo įrenginyje, kuris nepriklauso pareiškėjui, pareiškėjo vardu susikūrė kitą „Smart-ID" paskyrą. Taip tretieji asmenys įgijo galimybę pareiškėjo vardu prie pareiškėjo interneto banko ir kartu sąskaitos jungtis iš kito įrenginio ir pareiškėjo vardu inicijuoti bei tvirtinti veiksmus ir operacijas (tvirtinti mokėjimus, atidaryti sąskaitas, keisti operacijų limitus, peržiūrėti likučius, sudaryti sutartis, teikti prašymus ir pan.).

2021 m. spalio 19 d. 19 val. 26 min. bankas SMS žinute pareiškėjo telefono numeriu informavo pareiškėją apie pareiškėjo vardu sukurtą naują „Smart-ID" paskyrą: *„Gerb. Kliente, Jūsų vardu SEB banke registruojama „Smart-ID Basic" paskyra. Jei to neinicijavote, prašom kuo skubiau susisiekti tel. +370 5 268 2800. SEB bankas.*"

2021 m. spalio 19 d. 19 val. 37 min. tretieji asmenys, pasinaudodami naujai sukurta „Smart-ID" paskyra, prisijungė prie pareiškėjo interneto banko ir pareiškėjo vardu naudodamiesi naujai sukurta „Smart-ID" paskyra patvirtino šiuos veiksmus: 2021 m. spalio 19 d. 19 val. 38 min. inicijavo 3 800 Eur mokėjimo operaciją iš pareiškėjo banko sąskaitos Nr. LT *duomenys neskelbiami* ; 2021 m. spalio 19 d. 19 val. 40 min. atidarė naują banko sąskaitą LT *duomenys neskelbiami* ; 2021 m. spalio 19 d. 19 val. 41 min. pateikė prašymą pakeisti naujai atidarytos banko sąskaitos mokėjimo operacijų dienos ir mėnesio limitus (nustatė 4 000 Eur dienos ir 4 000 Eur mėnesio limitus); 2021 m. spalio 19 d. 19 val. 46 min. iš naujai atidarytos banko sąskaitos (iš sąskaitos Nr. LT *duomenys neskelbiami*) inicijavo 3

800 Eur mokėjimo operaciją.

Išnagrinėjęs pareiškėjo prašymą grąžinti neautorizuotų mokėjimo operacijų lėšas, bankas pateikė pareiškėjui atsakymą, kad bankas pareiškėjui negrąžins mokėjimo operacijų lėšų.

Nesutikdamas su banko atsakymu, pareiškėjas kreipėsi į Lietuvos banką dėl ginčo nagrinėjimo. Kreipimesi į Lietuvos banką pareiškėjas paaiškino, kad iš jo sąskaitos banke buvo įvykdyta jam priklausančių piniginių lėšų vagystė, už ją yra atsakingas bankas. Pareiškėjas paaiškino, kad į savo telefoną gavo SMS žinutę, įterptą į tikrų banko žinučių srautą, joje buvo pranešama, kad pareiškėjo paskyroje aptikta įtartina veikla, ir buvo prašoma paspausti SMS žinutėje pateiktą aktyvią nuorodą. Paspaudęs šią nuorodą, pareiškėjas pateko į interneto puslapį, vizualiai panašų į banko interneto puslapį, ir jame suvedė savo personalizuotus saugos duomenis (asmens kodą, banko atpažinimo kodą), taip pat savo mobiliajame įrenginyje suvedė „Smart-ID" PIN1 ir PIN2 kodus neįtardamas jokios apgaulingos veiklos. Pareiškėjas paaiškino, kad, atlikęs šiuos veiksmus, gavo banko SMS žinutę, kad pareiškėjo vardu yra užregistruota naujai sukurta „Smart-ID" paskyra. Minėtoje žinutėje buvo nurodoma, kad jeigu šio veiksmo pareiškėjas pats neinicijavo, turėtų kuo skubiau susisiekti su banku. Pareiškėjas teigia, kad nedelsdamas prisijungė prie savo banko sąskaitos ir pamatė, kad lėšos iš jos dar nebuvo nurašytos. Pareiškėjas teigė nepastebėjęs jokių su jo sąskaita susijusių įtartinų veiksmų. Tuomet pareiškėjas telefonu kreipėsi į banką ir pranešė apie gautą SMS žinutę apie įtartiną veiklą jo banko sąskaitoje. Banko darbuotojas telefonu pareiškėją informavo, kad iš jo sąskaitos Nr. LT *duomenys neskelbiami* yra įvykdyta 3 800 Eur mokėjimo operacija. Pareiškėjas teigia, kad banko darbuotoją informavo, kad šios mokėjimo operacijos pats neinicijavo, ir prašė sustabdyti šios mokėjimo operacijos vykdymą. Pareiškėjo nuomone, bankas privalėjo šią mokėjimo operaciją sustabdyti ir jos nevykdyti, tačiau dėl banko darbuotojo neveiklumo mokėjimo operacijos nebuvo sustabdytos, nors tada, kai buvo telefonu kalbamasi su banko darbuotoju, lėšos iš pareiškėjo banko sąskaitos dar nebuvo nurašytos.

Papildomai pareiškėjas teigė, kad jo banko sąskaitos Nr. LT *duomenys neskelbiami* nustatytas dienos operacijų limitas buvo 1 500 Eur, tačiau bankas įvykdė dvi po 3 800 Eur mokėjimo operacijas ir taip pažeidė pareiškėjo ir banko susitarimo dėl mokėjimo operacijų limito sąlygas. Be to, bankas neužtikrino mokėjimo sistemų saugumo ir lėšos iš pareiškėjo banko sąskaitos galėjo būti pavogtos dalyvaujant banko darbuotojams. Pareiškėjas taip pat mano, kad bankas neapsaugojo savo naudojamų telefono ryšio kanalų nuo pašalinių trečiųjų asmenų ar neteisėtų banko darbuotojų veiksmų.

Pareiškėjas prašė išreikalauti iš banko su mokėjimo operacijų įvykdymu susijusius įrodymus ir grąžinti pareiškėjui įvykdytų mokėjimo operacijų lėšas – 7 600 Eur.

Bankas nesutinka tenkinti pareiškėjo reikalavimo. Atsiliepime bankas nurodė atlikto tyrimo metu nustatytas mokėjimo operacijų inicijavimo ir įvykdymo aplinkybes, kurios iš esmės sutampa su pareiškėjo nurodytomis mokėjimo operacijų inicijavimo aplinkybėmis. Banko teigimu, pareiškėjo veiksmai, dėl kurių jis prarado savo mokėjimo priemonę, turėjo didelio neatsargumo požymių. Pareiškėjas dėl savo didelio neatsargumo neįgyvendino Lietuvos Respublikos mokėjimų įstatymo 34 straipsnyje aptartų mokėjimo paslaugų vartotojo pareigų, susijusių su naudojimosi mokėjimo priemone ir personalizuotais saugumo duomenimis, neišsaugojo personalizuotų saugos duomenų, tai lėmė, kad pareiškėjas prarado mokėjimo priemonę, o tretieji asmenys įgijo galimybę pareiškėjo vardu inicijuoti mokėjimo operacijas. Pareiškėjas nesilaikė ir banko Bendrųjų paslaugų teikimo taisyklių (toliau – Taisyklės) 1 priedo 10 skyriuje nustatytų reikalavimų saugoti banko suteiktą mokėjimo priemonę ir su ja susijusius personalizuotus saugumo duomenis ir imtis visų reikiamų veiksmų, kad personalizuoti saugumo duomenys nebūtų atskleisti kitiems asmenims. Taip pat pareiškėjas nesilaikė ir banko Paslaugų interneto banke teikimo sąlygų aprašo (toliau – Aprašas) 20.4.4 papunktyje ir 38^5 punkte nustatytų mokėjimo priemonės savininko pareigų: saugoti atpažinimo priemones, nedelsiant informuoti banką apie šių priemonių praradimą ar slaptumo pažeidimą, laikyti paslaptyje banko atpažinimo kodą, slaptažodžius, PIN kodus, neužrašyti jų ant generatoriaus ar kitų kartu su juo laikomų daiktų ir jokia kita forma neatskleisti ar nepadaryti jų prieinamų tretiesiems asmenims.

Bankas teigia, kad, įvertinęs pareiškėjo elgesį, mano, kad pareiškėjas elgėsi itin neapdairiai ir neatsargiai: paspaudė neaiškią nuorodą, suvedė savo interneto banko atpažinimo kodą, asmens kodą ir savo mobiliajame įrenginyje savo atliekamus veiksmus patvirtino suvesdamas tik jam žinomus jo žinioje esančios „Smart-ID" paskyros PIN1 ir PIN2 kodus, dėl to yra pagrindas pareiškėjui taikyti Mokėjimų įstatymo 39 straipsnio 3 dalies nuostatą, kad mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai, jeigu jis juos patyrė veikdamas nesąžiningai arba tyčia ar dėl didelio neatsargumo neįvykdęs vienos ar kelių

šio įstatymo 34 straipsnyje nustatytų pareigų.

Banko teigimu, pareiškėjas galėjo lengvai suprasti ir įvertinti savo atliekamų veiksmų reikšmę ir pasekmes, nes tokius veiksmus atliko ne pirmą kartą – „Smart-ID" programėle, kaip atpažinimo priemone, naudojasi nuo 2019 metų, daug kartų yra jungęsis prie interneto banko, tvirtinęs mokėjimo nurodymus, todėl turėjo nesunkiai suprasti, kad interneto banko atpažinimo kodas, asmens kodas ir „Smart-ID" PIN1 ir PIN2 kodai yra naudojami jungtis prie interneto banko mokėjimo nurodymams tvirtinti ir kitiems veiksmams interneto banke atlikti, ir turėjo kritiškai įvertinti, ar saugu suvesti minėtus duomenis, nes žinojo, kad pats mokėjimo operacijų neinicijavo.

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

Bankas atsiliepime taip pat teigė, kad pareiškėjo didelį neatsargumą įrodo ir aplinkybė, kad pareiškėjo iš trečiųjų asmenų SMS žinute gauta aktyvi nuoroda, kurią pareiškėjas buvo raginamas paspausti, niekaip nebuvo susijusi su banku, joje netgi nebuvo jokios nuorodos į banko pavadinimą. Ir nors bankas pripažįsta, kad iš trečiųjų asmenų gauta SMS žinutė buvo įterpta į tikrų banko žinučių srautą ir galėjo pareiškėją suklaidinti, tačiau, banko nuomone, pareiškėjas turėjo ir galėjo kreiptis į banką, kad šias abejones išsklaidytų. Bankas paaiškino, kad nors SMS žinutė nebuvo siunčiama iš banko, tačiau, atsižvelgiant į pasirinktus nustatymus, mobilieji telefonai žinutes gali grupuoti pagal siuntėjo vardą. Bankas papildomai atkreipė dėmesį į tai, kad nesiunčia SMS žinučių su prašymu paspausti žinutės tekste pateiktą aktyvią nuorodą, kuri nukreipia į banko interneto banką.

Dėl pareiškėjo teiginio, kad bankas turėjo sustabdyti mokėjimo operacijas ir jų nevykdyti, bankas paaiškino, kad banko darbuotojas telefoninio pokalbio su pareiškėju metu neturėjo galimybės sustabdyti mokėjimo operacijų, nes mokėjimo nurodymai buvo pateikti iki sąskaitos blokavimo ir šie mokėjimo nurodymai buvo momentiniai, tai reiškia, kad mokėjimo operacijų lėšų gavėjui pervedimas trunka vos 10 sekundžių. Bankas pažymėjo, kad kreipėsi į lėšų gavėjo mokėjimo paslaugų teikėją dėl lėšų sugrąžinimo, tačiau sugrąžinti mokėjimo operacijų lėšų nepavyko.

Dėl pareiškėjo argumento, kad mokėjimo operacijos galėjo būti įvykdytos dėl banko darbuotojų neteisėtų veiksmų, pasireiškusių sukčiavimu, bankas pažymėjo, kad, atlikęs vidinį tyrimą, jokių banko darbuotojų neteisėtų veiksmų nenustatė.

Atsiliepime 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. Lietuvos bankas ginčo nagrinėjimo proceso metu neatlieka Lietuvos Respublikos Lietuvos banko įstatymo 42^1 straipsnyje reglamentuotų patikrinimų, skirtų faktinėms aplinkybėms, susijusioms su Lietuvos banko priežiūrimo finansų rinkos dalyvio galimu Lietuvos banko kompetencijai priskirtų teisės aktų reikalavimų pažeidimu, nustatyti ir įvertinti. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Pareiškėjo ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjui pareiškėjo vardu banke atidarytose sąskaitose atliktų mokėjimo operacijų lėšas, iš viso – 7 600 Eur. Pareiškėjas teigia neautorizavęs mokėjimo operacijų, tačiau ir neneigia trečiųjų asmenų suklastotame banko interneto puslapyje pats suvedęs savo prisijungimo prie banko paskyros duomenis ir savo mobiliajame telefone suvedęs „Smart-ID" PIN1 ir PIN2 kodus. Pareiškėjo teigimu, tretieji asmenys be jo žinios ir sutikimo įgijo galimybę iš jo banko sąskaitos įvykdyti mokėjimo operacijas, nes bankas neužtikrino mokėjimo sistemų ir naudojamų telefono ryšio kanalų saugumo. Pareiškėjo teigimu, lėšų vagystė iš jo banko sąskaitos galėjo būti įvykdyta dėl neteisėtų banko darbuotojų veiksmų. Be to, bankas privalėjo nevykdyti pareiškėjo neautorizuotų mokėjimo operacijų – jas stabdyti ir atšaukti jų vykdymą, tačiau to nepadarė, todėl turi atlyginti pareiškėjo patirtus nuostolius. Bankas teigia, kad pareiškėjo mokėjimo operacijos buvo patvirtintos šalių sutarta forma ir tvarka, dėl to bankas jas pagrįstai įvykdė. Taip pat bankas teigia, kad yra sąlygos pareiškėjo elgesį, prarandant savo mokėjimo priemonę, vertinti kaip labai neatsargų, todėl bankas mano, kad neturi pareigos kompensuoti pareiškėjui jo patirtų nuostolių dėl mokėjimo operacijų įvykdymo. Dėl šių priežasčių, banko nuomone, visi mokėjimo operacijų nuostoliai turėtų tekti pareiškėjui.

Tarp šalių nėra ginčo, kad mokėjimo operacijoms įvykdyti nebuvo duotas pareiškėjo sutikimas, t. y. tiek pareiškėjas, tiek bankas pripažįsta, kad mokėjimo operacijas inicijavo ne pats pareiškėjas, o tretieji asmenys, neteisėtu būdu pasisavinę pareiškėjo mokėjimo priemonę. Atsiliepime bankas iš esmės remiasi Mokėjimų įstatymo nuostatomis, reglamentuojančiomis mokėtojo atsakomybę už neautorizuotas mokėjimo operacijas. Taigi, galima daryti išvadą, kad bankas pripažįsta, kad mokėjimo operacijos nagrinėjamo ginčo atveju laikytinos neautorizuotomis. Taip pat svarbu tai, kad ginčo byloje ginčo šalių pateikti paaiškinimai bei banko pateikti vidaus sistemų duomenys apie mokėjimo operacijų įvykdymą leidžia teigti, kad mokėjimo operacijas inicijavo ne pats pareiškėjas, bet tretieji asmenys, neteisėtu būdu pasisavinę pareiškėjo mokėjimo priemonę. Atsižvelgiant į tai, kad iš esmės abi ginčo šalys sutaria, kad mokėjimo operacijos galėjo būti inicijuotos be pareiškėjo žinios ir sutikimo, bei į tai, kad ginčo byloje turimi banko sistemų duomenys leidžia teigti, kad mokėjimo operacijas inicijavo ne pats pareiškėjas, toliau sprendime nebus analizuojamos su mokėjimo operacijų autorizavimo vertinimu susijusios aplinkybės, o mokėjimo operacijos laikomos pareiškėjo neautorizuotomis.

Ginčo šalys iš esmės nesutaria dėl to, kam turėtų tekti atsakomybė už neautorizuotų mokėjimo operacijų įvykdymą: bankas teigia, kad pareiškėjo elgesys, tretiesiems asmenims atskleidžiant savo personalizuotus saugos duomenis ir prarandat savo mokėjimo priemonę, buvo labai neatsargus, pareiškėjas teigia, kad lėšas prarado dėl banko mokėjimų sistemos saugumo trūkumų bei galimai neteisėtų banko darbuotojų veiksmų. Taip pat pareiškėjas teigia, kad bankas turėjo pareiškėjo mokėjimo operacijų nevykdyti ir jas atšaukti, o kadangi to nepadarė, turi atlyginti pareiškėjo patirtus nuostolius.

Siekiant išspręsti tarp pareiškėjo ir banko kilusį ginčą, Lietuvos banko vertinimu, būtina nustatyti šias pagrindines aplinkybes: 1) ar bankas turėjo (turi) pareigą grąžinti pareiškėjui neautorizuotų mokėjimo operacijų sumas; 2) ar bankas turėjo pareigą nevykdyti jam pateiktų mokėjimo nurodymų; 3) ar bankas turėjo pareigą atšaukti mokėjimo operacijas.

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

Dėl neautorizuotų mokėjimo operacijų pasekmių ir pareiškėjo teisės į mokėjimo operacijų sumų grąžinimą

Vadovaudamasis Mokėjimų įstatymo 38 straipsnio 1 dalimi, mokėtojo mokėjimo paslaugų teikėjas privalo grąžinti mokėtojui neautorizuotos mokėjimo operacijos sumą ne vėliau kaip iki kitos darbo dienos nuo sužinojimo apie tokios mokėjimo operacijos įvykdymą,

išskyrus atvejus, kai mokėtojo mokėjimo paslaugų teikėjas turi pagrįstų priežasčių įtarti mokėtojo sukčiavimą ir apie šias priežastis raštu praneša priežiūros institucijai (Lietuvos bankui).

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

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

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

Kaip minėta, tiek pareiškėjo, tiek banko paaiškinimai apie mokėjimo operacijų įvykdymo aplinkybes iš esmės sutampa, o banko pateikti sistemų išrašai patvirtina ginčo šalių pateiktus paaiškinimus apie mokėjimo operacijų įvykdymo aplinkybes.

Ginčo byloje nustatyta, kad pareiškėjas prarado savo prisijungimo prie banko paskyros personalizuotus saugos duomenis, kai prie paskyros jungėsi paspausdamas į savo mobiliųjį telefoną iš trečiųjų asmenų gautoje SMS žinutėje esančią aktyvią nuorodą ir taip pateko į netikrą banko interneto puslapį, vizualiai panašų į tikrąjį, jame suvedė savo banko atpažinimo kodą, asmens kodą ir prisijungimą prie savo paskyros iš kito, ne pareiškėjui priklausančio, įrenginio patvirtino suvesdamas „Smart-ID" PIN1 ir PIN2 kodus. Šiuos duomenis nusavino tretieji asmenys ir savo mobiliojo telefono įrenginyje pareiškėjo vardu sukūrė naują „Smart-ID" paskyrą. Tretieji asmenys naudodamiesi pareiškėjo vardu sukurta naują „Smart-ID" paskyra iš pareiškėjo sąskaitos Nr. LT *duomenys neskelbiami* inicijavo 3 800 Eur mokėjimo operaciją gavėjui. Taip pat tretieji asmenys pareiškėjo vardu atidarė naują banko sąskaitą Nr. L *duomenys neskelbiami* ir pateikė prašymą nustatyti naujai atidarytos banko sąskaitos mokėjimo operacijų dienos ir mėnesio limitus (nustatė 4 000 Eur dienos ir 4 000 Eur mėnesio limitus). Atlikę šiuos veiksmus, tretieji asmenys iš šios pareiškėjo vardu atidarytos naujos banko sąskaitos inicijavo dar vieną 3 800 Eur mokėjimo operaciją gavėjui.

Pagal ginčo byloje pareiškėjo pateiktus paaiškinimus, spausdamas trečiųjų asmenų jam atsiųstoje SMS žinutėje pateiktą aktyvią nuorodą ir vesdamas savo banko atpažinimo kodą, asmens kodą ir „Smart-ID" PIN1 bei PIN2 kodus, pareiškėjas manė, kad tokiais savo veiksmais siekia išvengti neteisėtų trečiųjų asmenų veiksmų jo banko sąskaitoje. Ginčo byloje nustatytais duomenimis, pareiškėjas iš trečiųjų asmenų gavo SMS žinutę su tokiu tekstu: *„Jusu paskyroje aptikta itartinos veiklos, spustelekite sia nuoroda, kad to isvengtume: HK32937.com."* Pareiškėjas teigia, kad ši žinutė jam nesukėlė jokių įtarimų, nes buvo įsiterpusi į tikrų jam banko siųstų SMS žinučių srautą, todėl jis pagrįstai manė, kad vykdo banko jam pateiktus nurodymus.

Teigdamas, kad pareiškėjo elgesys, dėl kurio jis prarado savo mokėjimo priemonę, turi didelio neatsargumo požymių, bankas remiasi tuo, kad pareiškėjas nesilaikė mokėtojui nustatytos pareigos saugoti personalizuotus saugos duomenis ir niekam jų neatskleisti. Banko teigimu, pareiškėjas paspaudė trečiųjų asmenų atsiųstą aktyvią nuorodą, nors ji vizualiai nebuvo panaši į su banku galimą sieti nuorodą, joje nebuvo net užuominos į banko pavadinimą. Tai pareiškėjui nekėlė jokių įtarimų ir jis paspaudė jam atsiųstą aktyvią nuorodą net neįsitikinęs, ar ji atitinka banko interneto banko svetainės adresą, kuriuo jis įprastai prisijungdavo ir inicijuodavo mokėjimo operacijas interneto banke. Pareiškėjas, net ir gavęs SMS žinutę iš banko, kad jo vardu yra sukurta nauja „Smart-ID" paskyra, nedelsdamas nesikreipė į banką,

nors pats naujos „Smart-ID“ paskyros sukūrimo neinicijavo.

Lietuvos bankas pažymi, kad didelis neatsargumas ar paprastas neatsargumas yra vertinamojo pobūdžio aplinkybės, todėl išvada dėl mokėtojo elgesio vertinimo kaip neatsargaus ar labai neatsargaus dėl neautorizuotos mokėjimo operacijos ar dėl mokėjimo priemonės praradimo, lėmusio neautorizuotą mokėjimo operaciją, darytina kiekvienu konkrečiu atveju, įvertinus nustatytų individualių, specifinių aplinkybių visumą, kurią patvirtina ginčo byloje esantys įrodymai ir (arba) yra šalių neginčijamos neautorizuotos mokėjimo operacijos įvykdymo aplinkybės. Taigi, išvada dėl mokėtojo paprasto ar didelio neatsargumo, kaip vertinamojo pobūdžio aplinkybė, negali būti daroma izoliuotai, išsamiai neįvertinus viso neautorizuotos mokėjimo operacijos įvykdymo ir su juo susijusių aplinkybių konteksto.

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

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

Vertinant, ar pareiškėjo elgesys, kai jis paspaudė į mobilųjį telefoną atsiųstoje SMS žinutėje esančią aktyvią nuorodą jo ir nepastebėjo, kad pateko į trečiųjų asmenų suklastotą banko interneto puslapį ir jame suvedė savo banko atpažinimo kodą, asmens kodą, o vėliau savo mobiliajame telefone „Smart-ID“ PIN1 bei PIN2 kodus, gali būti vertinamas kaip labai neatsargus pareiškėjo elgesys, t. y. toks elgesys, dėl kurio mokėjimo priemonės turėtojo veiksmai iš esmės skiriasi nuo atsargaus elgesio reikalavimų, pažymėtina, kad vien tik faktas, kad pareiškėjas paspaudė jam SMS žinute atsiųstą aktyvią nuorodą ir nepastebėjo, kad pateko ne į tikrą banko interneto puslapį, o į trečiųjų asmenų suklastotą banko interneto puslapį, savaime nereiškia pareiškėjo didelio neatsargumo. Nagrinėjamo ginčo atveju pareiškėją objektyviai galėjo suklaidinti ir kartu sumažinti jo budrumą tas faktas, kad pareiškėjas SMS žinutę su aktyvia nuoroda gavo įterptą į kitų tikrų jam anksčiau banko siųstų žinučių srautą. Tačiau nagrinėjamo ginčo atveju atkreiptinas dėmesys, kad vis dėlto trečiųjų asmenų pareiškėjui atsiųstoje SMS žinutėje pateikta aktyvi nuoroda tikrąją banko interneto banko nuorodą nebuvo panaši – pateiktos nuorodos pavadinime nebuvo jokio panašumo į jungiantis prie banko interneto banko matomos informacijos (pvz., nurodytas klaidingas banko pavadinimas, kuris vizualiai gali atrodyti panašus į tikrąjį banko pavadinimą ir pan.), be to, SMS žinutėje pateikta informacija buvo parašyta ne lietuvių abėcėles raidėmis, todėl pareiškėjas, jeigu tik būtų buvęs pakankamai atidus bei kritiškas SMS žinute gautos informacijos atžvilgiu, galėjo pastebėti, kad pateiktos nuorodos pavadinime nėra jokių su prisijungimo prie banko interneto puslapio galimų susieti duomenų ir kad jam neva iš banko atsiųstoje SMS žinutėje informacija pateikiama ne lietuvių abėcėlės raidėmis. Tačiau, kaip ir minėta, atsižvelgiant į tai, kad trečiųjų asmenų SMS žinutė su aktyvia nuoroda buvo įterpta į tikrų banko žinučių srautą, taip pat į tai, kad, pareiškėjo pateiktais duomenimis, bankas vis dėlto anksčiau pareiškėjui yra siuntęs SMS žinutę su aktyvia nuoroda, vertintina, kad pareiškėjui pagrįstai galėjo atrodyti, kad SMS žinutę siuntė pats bankas ir dėl to pareiškėjo budrumas galėjo būti sumažėjęs.

Vertinant tolimesnius pareiškėjo veiksmus pareiškėjui paspaudus aktyvią nuorodą ir patekus į trečiųjų asmenų suklastotą interneto banko puslapį, kuris vizualiai atrodė panašus į tikrąjį banko interneto puslapį, visų pirma pažymėtina, kad pareiškėjas SMS žinute iš trečiųjų asmenų gavo pranešimą, kad jo paskyroje yra aptikta įtartina veikla, ir būtent siekdamas išvengti neteisėtų trečiųjų asmenų veiksmų jo banko sąskaitoje, pareiškėjas jungėsi prie savo banko paskyros, suvesdamas tokiam prisijungimui reikalingus personalizuotus saugos duomenis. Atkreiptinas dėmesys, kad, norint prisijungti prie paskyros, reikia suvesti banko atpažinimo kodą, asmens kodą ir savo tapatybę patvirtinti suvedant „Smart-ID“ PIN1 kodą. Šių duomenų pakanka tam, kad patektum į savo banko paskyrą. Tačiau pareiškėjo papildomai dar buvo prašoma suvesti ir „Smart-ID“ PIN2 kodą, kuris iš esmės yra skirtas. mokėjimo operacijai

patvirtinti ir atitinka elektroninį parašą. Tačiau pareiškėjui tai nesukėlė jokių įtarimų ir jis atliko visus trečiųjų asmenų jo prašomus atlikti veiksmus – suvedė visus personalizuotus saugos duomenis, įskaitant ir „Smart-ID" PIN2 kodą, nors neturėjo tikslo patvirtinti mokėjimo operacijos arba kitų veiksmų, o turėjo tikslą tik prisijungti prie savo banko paskyros.

Analizuojamų aplinkybių kontekste svarbu įvertinti ir tai, ar pareiškėjas, suvesdamas „Smart-ID" PIN1 ir PIN2 kodus, galėjo suprasti, kad atlieka veiksmus, kurie gali lemti tam tikras teisines pasekmes, šiuo atveju – mokėjimo priemonės praradimą ir neautorizuotos mokėjimo operacijos iš jo banko sąskaitos įvykdymą. Banko Taisyklių 1 priedo 3 punkte nėra įvardyta, kurio „Smart-ID" PIN kodo (PIN1 ar PIN2) suvedimas banko ir pareiškėjo santykiuose yra laikytinas sutikimo, kad iš pareiškėjo banko sąskaitos būtų atlikta mokėjimo operacija, davimu arba kad „Smart-ID" PIN kodo (PIN1 ar PIN2) suvedimas naudotinas, siekiant atlikti veiksmus, susijusius su turima tapatybės patvirtinimo priemone (taigi, pačia „Smart-ID" paskyra mobiliajame įrenginyje) ir (ar) jos pakeitimu. Tokia informacija plačiau atskleidžiama banko interneto svetainėje adresu *https://www.seb.lt/privatiems/el-bankininkyste/paslaugos-internetu/prisijungimo-priemones-smart-id-m-parasas*. Pateiktos nuorodos skiltyje „Smart-ID lygmenys ir galimybės" nurodoma, kad „Smart-ID" „gali būti naudojama norint saugiai prisijungti prie interneto banko, tvirtinti mokėjimus, naudotis trečiųjų šalių paslaugų teikėjų paslaugomis ir pasirašyti elektroninius dokumentus. Prilygsta elektroniniam parašui."

Vertinant, ar pareiškėjas galėjo pastebėti ir suprasti, kad prisijungimui prie jo banko paskyros yra prašoma suvesti personalizuotus saugos duomenis, kurie yra skirti ne tik prisijungti prie paskyros (banko atpažinimo kodas, asmens kodas ir „Smart-ID" PIN1 kodas), bet ir duomenis („Smart-ID" PIN2 kodą), kurie yra skirti mokėjimo operacijos įvykdymui patvirtinti, svarbu yra tai, kad pareiškėjas, banko pateiktais duomenimis, „Smart-ID" naudojasi nuo 2019 metų ir turėjo nemažai patirties, jungiantis prie paskyros naudojantis „Smart-ID", inicijuojant ir tvirtinant mokėjimo operacijas. Telefonu pareiškėjas Lietuvos bankui paaiškino, kad turėjo naudojimosi „Smart-ID" paskyra patirties ir jam yra tekę anksčiau suvesti „Smart-ID" PIN kodus, tiek tvirtinant mokėjimo operacijas, tiek norint pakeisti prisijungimo slaptažodžius.

Taigi, iš esmės pareiškėjui buvo žinoma, kad suvedus „Smart-ID" PIN2 kodą yra patvirtinamas mokėjimo operacijos iš jo banko sąskaitos įvykdymas arba patvirtinamas kitas konkretus veiksmas, kurį jis atlieka, tačiau, nepaisydamas to, pareiškėjas, iš esmės neturėdamas tikslo nei įvykdyti mokėjimo operaciją, nei patvirtinti kažkokį kitą veiksmą iš jo banko sąskaitos, o turėdamas tik tikslą prisijungti prie savo banko paskyros, suvedė ne tik duomenis, reikalingus prie paskyros prisijungti ir kuriuos jis įprastai atlikdavo jungdamasis prie savo banko paskyros, bet ir „Smart-ID" PIN2 kodą, kuris yra skirtas mokėjimo operacijoms ar kitiems pareiškėjo banko sąskaitoje atliekamiems veiksmams pavirtinti.

Lietuvos banko nuomone, jeigu pareiškėjas būtų buvęs pakankamai atidus ir kritiškas tiek SMS žinute gautos informacijos atžvilgiu, tiek ir savo atliekamų veiksmų atžvilgiu, būtų pastebėjęs, kad jo prašoma atlikti veiksmus, kurie nėra įprasti jungiantis prie savo paskyros, būtų pastebėjęs neįprastus ir įtartinus veiksmus ir, tikėtina, būtų nuo jų susilaikęs ir nedelsdamas būtų kreipęsis į banką dėl informacijos patikslinimo. Be to, ginčo byloje turimais duomenimis, tretiesiems asmenims pasinaudojus iš pareiškėjo neteisėtu būdu pasisavintais personalizuotais saugos duomenimis ir savo mobiliajame telefone pareiškėjo vardu sukūrus naują „Smart-ID" paskyrą, bankas pareiškėjui jo mobiliuoju telefono numeriu siuntė SMS žinutę, kurioje pareiškėją informavo, kad jo vardu buvo sukurta nauja „Smart-ID" paskyra, ir nurodė, kad jeigu pareiškėjas pats naujos paskyros sukūrimo neinicijavo, turi nedelsdamas kreiptis į banką telefonu (*„Gerb. Kliente, Jūsų vardu SEB banke registruojama „Smart-ID Basic" paskyra. Jei to neinicijavote, prašom kuo skubiau susisiekti tel. +370 5 268 2800. SEB bankas*"). Banko pateiktais duomenimis, pareiškėjas šią banko jam siųstą SMS žinutę gavo 2021 m. spalio 19 d. 19 val. 26 min., tačiau nedelsdamas nesikreipė į banką, o pagal pareiškėjo pateiktus paaiškinimus, pats jungėsi prie savo banko sąskaitos. Pareiškėjas telefonu į banką kreipėsi tik 19 val. 44 min., t. y. praėjus 18 min. nuo gautos banko žinutės apie naujos pareiškėjo vardu sukurtos „Smart-ID" paskyros sukūrimą. Ginčo byloje turimais duomenimis, tretieji asmenys pareiškėjo vardu iš pareiškėjo banko sąskaitos inicijavo pirmąją 3 800 Eur mokėjimo operaciją 19 val. 38 min. Taigi, jeigu pareiškėjas būtų buvęs pakankamai atidus ir rūpestingas ir gavęs banko SMS žinutę, kad jo vardu yra sukurta nauja „Smart-ID" paskyra, būtų nedelsdamas kreiptis į banką jam SMS žinutėje nurodytais kontaktais, labai tikėtina, kad pareiškėjas būtų išvengęs neautorizuotų mokėjimo operacijų iš jo banko sąskaitos įvykdymo.

Lietuvos banko nuomone, jeigu pareiškėjas būtų buvęs pakankamai atidus ir rūpestingas

ir būtų atkreipęs dėmesį į tai, kad prisijungimui prie jo paskyros buvo prašoma suvesti ir „Smart-ID" PIN2 kodą, kuris iš esmės yra skirtas mokėjimo operacijai patvirtinti, nors pareiškėjas turėjo nemažą naudojimosi „Smart- ID" patirtį, taigi, žinojo, kad „Smart-ID" paskyros PIN 2 kodas yra skirtas mokėjimo operacijoms tvirtinti arba kitiems veiksmams, atliekamiems jo banko sąskaitoje, tvirtinti, pareiškėjas būtų pastebėjęs įtartinus veiksmus ir nuo jų būtų susilaikęs, tačiau pareiškėjas elgėsi nerūpestingai ir toliau vykdė trečiųjų asmenų jam pateiktus nurodymus. Netgi gavęs banko SMS žinutę apie jo vardu sukurtą naują „Smart-ID" paskyrą, pareiškėjas delsė kreiptis į banką, dėl to iš esmės prarado galimybę blokuoti naudojimąsi savo paskyra dar iki tretiesiems asmenims inicijuojant mokėjimo operacijas. Taigi, Lietuvos banko vertinimu, pareiškėjas, jeigu tik būtų buvęs pakankamai atidus ir rūpestingas, galėjo pastebėti savo mokėjimo priemonės praradimą ir laiku užkirsti kelią neautorizuotų mokėjimo operacijų iš jo banko sąskaitos įvykdymui. Tačiau pareiškėjas elgėsi nerūpestingai ir, gavęs iš trečiųjų asmenų SMS žinutę, kad jo paskyroje yra aptikta įtartina veikla, nesikreipė į banką ir nepranešė bankui apie galimus neteisėtus trečiųjų asmenų veiksmus jo paskyroje, o priešingai, vykdė jam trečiųjų asmenų pateiktus nurodymus – suvedė personalizuotus saugos duomenis, reikalingus ne tik prie paskyros prisijungti, bet ir mokėjimo operacijoms iš banko sąskaitos patvirtinti, nors neturėjo tikslo įvykdyti mokėjimo operaciją. Netgi gavęs iš banko SMS žinutę, kad jo vardu yra sukurta nauja „Smart-ID" paskyra, pareiškėjas nekreipė dėmesio į banko raginimą nedelsiant kreiptis į banką, jeigu jis šių veiksmų pats neatliko. Lietuvos banko vertinimu, toks pareiškėjo elgesys gali būti pripažintas kaip elgesys, iš esmės besiskiriantis nuo atsargaus elgesio reikalavimų, kuris galiausiai ir lėmė, kad pareiškėjas prarado savo mokėjimo priemonę, o tretieji asmenys įgijo galimybę pareiškėjo vardu inicijuoti mokėjimo operacijas.

Mokėjimų įstatymo 34 straipsnyje reglamentuojamos mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigos: 1) naudotis mokėjimo priemone pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas; 2) sužinojus apie mokėjimo priemonės praradimą, vagystę arba neteisėtą pasisavinimą ar neautorizuotą jos naudojimą, nedelsiant apie tai pranešti mokėjimo paslaugų teikėjui arba jo nurodytam subjektui. Mokėjimo paslaugų vartotojas, gavęs mokėjimo priemonę, privalo imtis veiksmų, kad būtų apsaugoti personalizuoti saugumo duomenys (2 dalis). Taisyklių 1 priedo 10 skyriuje nurodoma, kad banko suteiktą mokėjimo priemonę ir su ja susijusius personalizuotus saugumo duomenis mokėtojas privalo saugoti ir imtis visų reikiamų veiksmų, kad personalizuoti saugumo duomenys nebūtų atskleisti jokiems kitiems asmenims. Taigi, įvertinus ginčo byloje turimus duomenis bei ginčo šalių paaiškinimus apie mokėjimo operacijų įvykdymo aplinkybes, galima teigti, kad pareiškėjas mokėjimo priemone naudojosi nesilaikydamas mokėjimo priemonės išdavimą ir naudojimą reglamentuojančių sąlygų, o sužinojęs apie neautorizuotą mokėjimo priemonės naudojimą (gavęs SMS žinutę apie įtartiną veiklą jo paskyroje, banko SMS žinutę apie naujos „Smart-ID" paskyros sukūrimą) nesikreipė į banką ir bankui nepranešė apie su jo mokėjimo priemone susijusius veiksmus, kurių jis pats neinicijavo, taigi, galima teigi, kad pareiškėjas neįvykdė Mokėjimų įstatymo 34 straipsnyje reglamentuojamų mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigų.

Visų ginčo byloje nustatytų aplinkybių kontekste galima daryti išvadą, kad pareiškėjo veiksmai, dėl kurių jis prarado mokėjimo priemonę, pasireiškė dideliu neatsargumu, tai galiausiai ir lėmė, kad buvo įvykdytos neautorizuotos mokėjimo operacijos iš pareiškėjo sąskaitos ir pareiškėjas patyrė nuostolių. Lietuvos banko nuomone, įvertinus pirmiau išdėstytas ginčo byloje nustatytas aplinkybes ir padarytas išvadas, galima teigti, kad pareiškėjas iki mokėjimo operacijų įvykdymo galėjo pastebėti, kad jo mokėjimo priemonę pasisavino tretieji asmenys. 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.

Vertinant Mokėjimų įstatymo nuostatas, reglamentuojančias atsakomybės už neautorizuotų mokėjimo operacijų įvykdymą pasiskirstymą, tam, kad bankas būtų atleistas nuo pareigos grąžinti neautorizuotų mokėjimo operacijų lėšas, turėtų būti nustatytas pareiškėjo sukčiavimas arba didelis neatsargumas. Kaip ir buvo minėta, Lietuvos banko nuomone, nagrinėjamo ginčo atveju pareiškėjo elgesys, dėl kurio jis prarado savo mokėjimo priemonę, gali būti laikomas labai neatsargiu, tai iš esmės ir lėmė neautorizuotų mokėjimo operacijų iš pareiškėjo sąskaitos įvykdymą. Įvertinus pirmiau išdėstytą informaciją, konstatuotina, kad yra pagrindas pareiškėjui taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, todėl pareiškėjo reikalavimas bankui grąžinti neautorizuotų mokėjimo operacijų lėšų sumą yra nepagrįstas ir

atmestinas.

Dėl banko pareigos grąžinti mokėjimo operacijos, įvykdytos po to, kai mokėtojas praneša apie mokėjimo priemonės praradimą ir neautorizuotą jos panaudojimą, lėšas

Pareiškėjas kreipimesi teigė, kad jam susisiekus su banku lėšos iš jo banko sąskaitos dar nebuvo nurašytos, todėl bankas turėjo galimybę nevykdyti pateiktų mokėjimo operacijų.

Mokėjimų įstatymo 39 straipsnio 5 dalyje nustatyta, kad „mokėtojas neturi patirti jokių nuostolių dėl prarastos, pavogtos ar neteisėtai pasisavintos mokėjimo priemonės po to, kai pateikia šio įstatymo 34 straipsnio 1 dalies 2 punkte nurodytą pranešimą, išskyrus atvejus, kai jis veikė nesąžiningai.“ Mokėjimų įstatymo 34 straipsnio 1 dalies 2 punkte nurodoma, kad mokėtojas, sužinojęs apie mokėjimo priemonės praradimą, vagystę arba neteisėtą pasisavinimą ar neautorizuotą jos naudojimą, nedelsdamas apie tai turi pranešti mokėjimo paslaugų teikėjui arba jo nurodytam subjektui. Mokėjimų įstatymo 39 straipsnio 6 dalyje nustatyta, kad „jeigu mokėjimo paslaugų teikėjas nesudaro sąlygų bet kuriuo metu pranešti apie prarastą, pavogtą arba neteisėtai pasisavintą mokėjimo priemonę, nuostoliai, atsiradę dėl mokėjimo priemonės neautorizuoto naudojimo, tenka mokėjimo paslaugų teikėjui, išskyrus atvejus, kai mokėtojas veikė nesąžiningai.“

Ginčo byloje nustatytais duomenimis, pareiškėjas savo mokėjimo priemonę prarado 2021 m. spalio 19 d. 19 val. 20 min., o į banką telefonu kreipėsi tą pačią dieną 19 val.44 min. Pirmoji mokėjimo operacija iš pareiškėjo banko sąskaitos buvo inicijuota dar iki pareiškėjui kreipiantis į banką – 2021 m. spalio 19 d. 19 val. 38 min., antroji mokėjimo operacija buvo inicijuota 19 val. 46 min. pareiškėjo pokalbio su banko darbuotoju metu, kai banko darbuotojas mėgino nustatyti pareiškėjo tapatybę. Taigi, pirma mokėjimo operacija buvo įvykdyta iki pareiškėjo kreipimosi į banką ir pranešimo apie mokėjimo priemonės paradimą ir neautorizuotą jos panaudojimą, o paskesnė mokėjimo operacija buvo įvykdyta pareiškėjui telefonu kalbantis su banko darbuotoju ir banko darbuotojui mėginant nustatyti pareiškėjo tapatybę.

Bankas pateikė pareiškėjo ir banko telefoninio pokalbio įrašą, iš kurio matyti, kad banko darbuotojas, pareiškėjui kreipusis į banką telefonu, mėgino nustatyti pareiškėjo tapatybę. Turimais duomenimis, šis pokalbis truko iš viso 15 min. Iš pateikto pokalbio įrašo matyti, kad banko darbuotojas prašė pareiškėjo pateikti duomenis, reikalingus pareiškėjo tapatybei nustatyti, ir informavo, kad iš pareiškėjo banko sąskaitos yra nurašytos lėšos. Banko darbuotojas šio pokalbio metu 19 val. 50 min. apribojo naudojimąsi pareiškėjo banko sąskaita. Taigi, nuo to, kai bankas nustatė pareiškėjo tapatybę ir apribojo naudojimąsi pareiškėjo sąskaita, praėjo tik keletas minučių. Objektyviai vertinant negalima teigti, kad toks laiko tarpas, kai buvo nustatyta pareiškėjo tapatybė, galėtų būti pripažintas kaip nepagrįstai ilgas delsimas. Be to, pareiškėjas mokėjimo priemonę buvo praradęs dar anksčiau, t. y. 19:20 val., tad tretieji asmenys iki pareiškėjui kreipiantis į banką jau buvo įgiję galimybę naudotis pareiškėjo sąskaita ir iš jos vykdyti mokėjimo operacijas.

Įvertinus pirmiau nustatytą informaciją, galima teigti, kad viena pareiškėjo neautorizuota mokėjimo operacija buvo įvykdyta tada, kai pareiškėjas pranešė apie mokėjimo priemonės paradimą ir neautorizuotą jos panaudojimą, o banko darbuotojas bandė nustatyti pareiškėjo tapatybę. Svarbu tai, kad, mokėjimo paslaugų teikėjui gavus jo paslaugų vartotojo pranešimą apie mokėjimo priemonės paradimą ir neautorizuotą jos panaudojimą, objektyviai yra reikalingas tam tikras laiko tarpas tam, kad būtų identifikuotas vartotojas ir būtų imtasi priemonių, kad būtų apribotas naudojimasis mokėjimo priemone. Nagrinėjamo ginčo atveju nėra pagrindo teigti, kad bankas nepagrįstai ilgai delsė apriboti naudojimąsi pareiškėjo sąskaita arba kad nesudarė pareiškėjui galimybių nedelsiant pranešti apie mokėjimo priemonės paradimą ir neautorizuotą jos panaudojimą. Taip pat nėra pagrindo teigti, kad pareiškėjo neautorizuota mokėjimo operacija buvo įvykdyta po to, kai buvo pranešta apie mokėjimo priemonės paradimą ir neautorizuotą jos panaudojimą, nes, kaip ir buvo minėta, ši mokėjimo operacija buvo įvykdyta tada, kai pranešimas buvo teikiamas ir buvo tikrinama informacija.

Dėl mokėjimo operacijų įvykdymo pagrįstumo bei mokėjimo nurodymų įvykdyti mokėjimo operacijas atšaukimo

Pareiškėjas teigė, kad bankas turėjo nevykdyti ir atšaukti mokėjimo operacijas, nes pokalbio su banko darbuotoju metu pareiškėjas banką informavo, kad mokėjimo operacijų pats neinicijavo.

Vertinant banko pareigos atšaukti mokėjimo operacijas vykdymą, pažymėtina, kad, pagal Mokėjimų įstatymo 44 straipsnio 1 dalies nuostatas, 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).

Remiantis ginčo byloje esančiais duomenimis, pareiškėjo prašymas atšaukti mokėjimo operacijas bankui buvo pateiktas po to, kai mokėjimo nurodymus jau buvo gavęs bankas, todėl Mokėjimų įstatyme nustatyta mokėjimo nurodymo atšaukimo terminas jau buvo praėjęs ir bankas atšaukti pareiškėjo vardu pateiktų mokėjimo nurodymų nebegalėjo. Bankas Lietuvos bankui paaiškino, kad, gavęs pareiškėjo prašymą atšaukti mokėjimo operacijas, kreipėsi į lėšų gavėją, tačiau jis nesutiko grąžinti lėšų, todėl bankas ir negalėjo pareiškėjui grąžinti lėšų.

Pareiškėjas taip pat teigė, kad vykdant mokėjimo operacijas jo banko sąskaitos Nr. LT *duomenys neskelbiami* dienos mokėjimo operacijų limitas buvo 1 500 Eur, todėl bankas turėjo nevykdyti dviejų 7 600 Eur mokėjimo operacijų.

Vertinant šio pareiškėjo pateikto teiginio pagrįstumą, pažymėtina, kad banko Lietuvos bankui pateikti įrodymai patvirtina, kad pareiškėjo banko sąskaitos Nr. LT *duomenys neskelbiami* dienos mokėjimo operacijų limitas mokėjimo operacijų inicijavimo metu buvo ne, kaip pareiškėjas teigia, 1 500 Eur, o 4 000 Eur. Todėl banko iš pareiškėjo banko sąskaitos Nr. LT *duomenys neskelbiami* įvykdyta 3 800 Eur mokėjimo operacija neviršijo nustatytų mokėjimo operacijų limitų. Kaip ir minėta, tretieji asmenys neteisėtu būdu pasisavinę pareiškėjo mokėjimo priemonę pareiškėjo vardu atidarė naują banko sąskaitą Nr. LT *duomenys neskelbiami* , nustatė 4 000 Eur mokėjimo operacijų limitą ir inicijavo dar vieną 3 800 Eur mokėjimo operaciją.

Taigi, Lietuvos bankui pateikti duomenys patvirtina, kad banko įvykdytos mokėjimo operacijos neviršijo banko sąskaitose nurodytų mokėjimo operacijų limitų, todėl nėra pagrindo teigti, kad bankas įvykdydamas mokėjimo operacijas pažeidė pareiškėjo ir banko susitarimo sąlygas.

Atsižvelgiant į tai, kas buvo išdėstyta pirmiau, nėra pagrindo vertinti, kad bankas nepagrįstai įvykdė mokėjimo operacijas ir kad nepagrįstai jų neatšaukė.

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

Atmesti pareiškėjo X.X. reikalavimą.

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

[Pareigų pavadinimas] [Vardas ir pavardė]