Projektas
Ginčo byla Nr. 2021-02757

LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

SPRENDIMAS DĖL X. X. IR „SWEDBANK", AB, GINČO NAGRINĖJIMO

2021 m. gruodžio 23 d. Nr. 429-465
Vilnius

Lietuvos bankas gavo X. X. (toliau – pareiškėja) kreipimąsi, kuriuo prašoma išnagrinėti tarp pareiškėjos ir „Swedbank", AB, (toliau – bankas) kilusį ginčą.

N u s t a t y t a:

2021 m. rugsėjo 8 d. 20:29 val. pareiškėja lankėsi degalinėje ir banko išduota mokėjimo kortele davė sutikimą 60 Eur operacijai, kurios sumą prekybininkas 20:33 val. pakoregavo atsižvelgdamas į faktiškai įsigytų degalų kiekį. Po to, kai pareiškėja patikrino (20:36 ir 20:43 val.), ar degalinėje ji atsiskaitė už sumą, už kurią faktiškai įsigijo degalų, t. y. praėjus daugiau kaip pusvalandžiui po paskutinės sesijos pabaigos, jos telefone aktyvavosi Paskyros Nr. 1 ekranas[1] – apie 21:20 val. pareiškėja savo telefono ekrane pamatė, kaip aktyvavosi jos „Smart-ID" programėlė, kurioje pareiškėja suvedė Paskyrai Nr. 1 taikomus slaptažodžius PIN1 ir PIN2.

2021 m. rugsėjo 8 d., 21:27:30 val. ir 21:28:59 val., pareiškėjos vardu atidarytoje banko sąskaitoje Nr. (*duomenys neskelbtini*) (toliau — Sąskaita) pareiškėjos vardu buvo duoti sutikimai įvykdyti du momentinius kredito pervedimus SEPA gavėjui, kurių bendra suma – 7 700 Eur, gavėjui Y. Y. į jo sąskaitą Nr. (*duomenys neskelbtini*), atidarytą Revolut Payments UAB (toliau — Operacijos).

Sutikimas Operacijoms pareiškėjos vardu buvo duotas galiniame įrenginyje *iOS iPhone SE (iOS)*, IP adresas (*duomenys neskelbtini*), su pareiškėjos vardu skurta nauja „Smart-ID" paskyra Nr. (*duomenys neskelbtini*) (toliau — Paskyra Nr. 2). Paskyra Nr. 2 sukurta, panaudojant kitą, dar 2021 m. liepos 27 d. pareiškėjos susikurtą „Smart-ID" paskyrą Nr. (*duomenys neskelbtini*) (toliau – Paskyra Nr. 1), jos faktiškai valdomame galiniame įrenginyje *HUAWEI P20Pro (Android)*. Paskyra Nr. 2 pradėta kurti 21:20:26 val., o užbaigta 21:23:58 val. (blokuota tą pačią dieną 21:43:56 val.).

Pareiškėja, į savo telefoną gavusi žinutes, kad iš jos Sąskaitos atlikti kredito pervedimai (Operacijos), kurių ji pati neplanavo atlikti, paskambino į banką. Su pareiškėja bendravęs darbuotojas 2021 m. rugsėjo 8 d. 21:37:11 val. užblokavo pareiškėjos vardu išduotas mokėjimo priemones. Vėliau (t. y. 21:38 val.) pareiškėja buvo sujungta su kitu banko darbuotoju, kuris paprašė patikslinti Operacijų įvykdymo aplinkybes ir nurodė, kad informacija bus perduota atsakingiems banko darbuotojams, kurie imsis veiksmų, bandydami sugrąžinti Operacijų lėšas į pareiškėjos Sąskaitą.

Banko darbuotojai 2021 m. rugsėjo 9 d. ryte 7:46 ir 7:47 val. gavėjo mokėjimo paslaugų teikėjui pateikė sisteminį SEPA prašymą atšaukti Operacijas ir grąžinti jų lėšas mokėtojui (t. y. pareiškėjai), o tos pačios dienos 10:14 ir 11:41 val. gavo gavėjo mokėjimo paslaugų teikėjo atsakymą, kad gavėjo sąskaitoje neliko lėšų.

2021 m. rugsėjo 13 d. pareiškėja pateikė prašymą bankui dėl Operacijų lėšų grąžinimo, į kurį bankas 2021 m. rugsėjo 14 d. pateikė neigiamą atsakymą.

Pareiškėja ginčija banko sprendimą nekompensuoti jai Operacijų lėšų. Pareiškėja kreipimesi nurodo, kad 2021 m. rugsėjo 8 d. apie 20:30 val. ji lankėsi degalinėje norėdama įsipilti degalų, tačiau siekiant atsiskaityti kortele, ji negalėjo ekrane pasirinkti norimos sumos ir įvesti PIN kodo, nes sistema, kaip būna įprastai tokiais atvejais, PIN kodo įvesti nereikalavo. Pareiškėja nurodo, kad grįžusi namo, ji prisijungė prie savo interneto banko ir patikrinusi

[1]Pareiškėjos paskutinė sesija prasidėjo 20:43:33 ir tęsėsi iki 20:47:37 val., o „Smart-ID" programėlėje prašymą suvesti Paskyros Nr. 1 Pin 1 pareiškėja gavo 21:20:26 val.

Sąskaitą pamatė, kad iš jos nurašyta 29 Eur suma už degalinėje įsigytus degalus. Pareiškėjos teigimu, tuo metu, kai ji buvo prisijungusi prie savo interneto banko, į jos telefoną buvo atsiųsta SMS žinutė su „Swedbank" logotipu ir inicialais, ir joje nurodyta, kad reikia atnaujinti duomenis „Smart-ID" programėlėje, kurią pareiškėja naudoja kaip tapatybės patvirtinimo priemonę. Kreipimesi nurodoma, kad pareiškėjai paspaudus pateiktą nuorodą, jos iškart buvo prašoma suvesti „Smart-ID" paskyros PIN1 ir PIN2. Pareiškėja kreipimesi dėsto, kad „programa veikė ilgai, atrodė, kad neužsikrauna", o tada pareiškėja gavo į savo el. paštą pranešimą, kad sukurtas „X. X. naujas ID". Pareiškėja nurodo, kad perskaičiusi laišką ir supratusi, kad neatliko jokių jame nurodytų veiksmų, t. y. nesukūrė naujos „Smart-ID" paskyros, nes to daryti neplanavo, pradėjusi ieškoti banko kontaktų, kad galėtų susisiekti su banko darbuotojais ir informuotų apie susidariusią situaciją, tačiau prisiskambinti nepavyko greitai, nes telefono linija buvo nuolat užimta. Tuo metu, kai, pareiškėjos teigimu, ji bandė susisiekti su klientų aptarnavimo specialistais, į jos telefoną atėjo žinutė apie tai, kad pareiškėja Y. Y. pervedė 5 500 Eur, o po to ir žinutė, kad pareiškėja gavėjui Y. Y. pervedė dar 2 200 Eur. Dėl šios priežasties pareiškėja nurodė iškart paskambinusi policijai, kurie patarė nedelsiant susisiekti su banku ir blokuoti mokėjimo priemones. Pareiškėja teigia bandžiusi tai padaryti, tačiau jos Sąskaita banke buvo blokuota tik po antrojo pokalbio su banko darbuotoju. Pareiškėja mano, kad bankas nesiėmė visų veiksmų, kad būtų užtikrintas jos lėšų, esančių banko Sąskaitoje, saugumas, todėl kreipimesi prašo rekomenduoti bankui grąžinti pareiškėjai dėl įvykdytų Operacijų iš jos Sąskaitos nurašytą 7 700 Eur sumą.

Bankas nesutinka tenkinti pareiškėjos reikalavimo. Bankas teigia siekiantis, kad tretieji asmenys banko vardu nesiųstų suklastotų pranešimų banko klientams, ir bendradarbiauja su telekomunikacijų bendrovėmis, kad šios nepraleistų SMS pranešimų, jei gavėjo, kuris nėra banko patvirtintas, pavadinime naudojamas banko vardas. Tačiau, banko teigimu, pasinaudojant šiuolaikinėmis technologijomis, SMS pranešimo siuntėjo pavadinimas gali būti nesudėtingai suklastojamas. Banko spėjimu, pranešime, kurį pareiškėja teigia gavusi iš banko (banko vardu), banko pavadinimas buvo nurodytas neteisingai, tačiau pareiškėja jo kritiškai nevertino ir besąlygiškai patikėjo pranešime nurodyta informacija tik dėl to, kad jame buvo naudojamas banko logotipas, kuriam suklastoti nereikia turėti jokių specialiųjų žinių. Bankas nurodo, kad pareiškėja turėjo paspausti pranešime esančią aktyvią nuorodą, kuri nukreipė pareiškėją į suklastotą interneto svetainę, kurioje pareiškėja suvedė savo asmens kodą ir naudotojo ID, kitaip pareiškėjos ekrane nebūtų aktyvavęsis Paskyros Nr. 1 ekranas su prašymu suvesti PIN 1, o po to ir PIN 2 kodą. Bankas pažymi, kad pareiškėja į banką paskambino po darbo valandų, kai vykdomi tik mokėjimo priemonių blokavimo veiksmai. Bankas nurodo, kad jam nėra žinoma, kiek laiko užtruko darbuotojas, kol užblokavo pareiškėjos mokėjimo priemones, pareiškėjai paskambinus į banką, tačiau atkreipia dėmesį, kad pareiškėja neginčija, kad tokie veiksmai būtų įvykdyti per nepagrįstai ilgą laiko tarpą. Bankas taip pat pažymėjo, kad Operacijos buvo įvykdytos kaip momentiniai mokėjimai – taigi, tretieji asmenys lėšomis gavėjo sąskaitoje įgijo galimybę disponuoti per keliolika sekundžių nuo mokėjimo nurodymų įvykdyti Operacijas patvirtinimo (taigi, dar iki pareiškėjai paskambinant į banką), todėl vertina, kad pareiškėja nepagrįstai tikėjosi, jog bankas galės atšaukti Operacijas, pareiškėjai kreipusis į banką, jau po jų įvykdymo. Bankas taip pat atkreipia dėmesį, kad kredito pervedimų atšaukimo paslaugą teikia tik darbo dienomis darbo valandomis ir tik tuomet, kai tokią galimybę turi – t. y. tik tuomet, jei kredito pervedimas dar nebūna išsiųstas iš banko.

Bankas taip pat nesutinka su pareiškėjos nuomone, kad jis nesiėmė visų veiksmų, kad būtų užtikrintas pareiškėjos lėšų Sąskaitoje saugumas. Banko teigimu, tretieji asmenys įgijo sąlygas inicijuoti Operacijas tik dėl to, kad pareiškėja dėl didelio neatsargumo sudarė visas sąlygas pasisavinti jos tapatybę ir jos vardu prisijungti bei inicijuoti Operacijas Sąskaitoje. Bankas taip pat pažymi, kad Operacijos neatitiko kriterijų, dėl kurių galėtų būti stabdomos mokėjimo operacijos, vykdant pinigų plovimo ir teroristų finansavimo prevencijos reikalavimus, todėl bankas nurodo neturėjęs jokio pagrindo (teisėtų priežasčių) nevykdyti Operacijų, nes sutikimo Operacijoms davimo metu pareiškėjos tapatybė buvo patvirtinta taikant sustiprintą tapatybės nustatymo procedūrą. Griežta (saugesnio) tapatybės patvirtinimo procedūra buvo taikoma ir sukuriant Paskyrą Nr. 2, naudojantis pačios pareiškėjos turima tapatybės patvirtinimo priemone – Paskyra Nr. 1.

Išvengti nuostolių, banko teigimu, pareiškėja turėjo galimybę, jei būtų kritiškai vertinusi matomą informaciją ir atsižvelgusi į banko viešai skelbiamas saugaus naudojimosi el. paslaugomis rekomendacijas, kurios yra neatskiriama pareiškėjos su banku sudarytos elektroninių paslaugų teikimo sutarties dalis. Minėtos elektroninių paslaugų teikimo sutarties

nuostatos taip pat įtvirtina pareiškėjos, kaip mokėjimo paslaugų vartotojos, pareigą užtikrinti jos turimų tapatybės patvirtinimo priemonių personalizuotų saugumo duomenų konfidencialumą. Bankas mano, kad pareiškėjos didelis neatsargumas pasireiškė ir tuo, kad jai buvo būtina įsitikinti, ar per SMS atsiųstą nuorodą atsidaro tikras, o ne suklastotas banko svetainės puslapis, nes tai – viena iš esminių atidaus ir rūpestingo elgesio standartą atitinkančių saugaus elgesio internete, vykdant finansines operacijas, taisyklių, o aplinkybė, kad pareiškėja neperskaitė programėlėje „Smart-ID" (Paskyroje Nr. 1) veiksmo, kuriam duoda sutikimą, suvesdama PIN kodus, aprašymo, rodo pareiškėjos didelį neatsargumą. Banko vertinimu, dėl nurodytų priežasčių, t. y. atsižvelgiant į tai, kad nuostolių pareiškėja patyrė dėl didelio neatsargumo, banko atsisakymas kompensuoti pareiškėjos nuostolius dėl Operacijų įvykdymo yra pagrįstas, todėl pareiškėjos reikalavimas atmestinas.

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 (toliau – Taisyklės) 45 punktu, vartojimo ginčai Lietuvos banke nagrinėjami laikantis rungimosi, ginčų nagrinėjimo operatyvumo, koncentracijos, ekonomiškumo ir bendradarbiavimo principų. Vartotojas ir finansų rinkos dalyvis privalo įrodyti tas aplinkybes, kuriomis remiasi kaip savo reikalavimų arba atsikirtimų pagrindu, išskyrus atvejus, kai remiamasi aplinkybėmis, kurių nereikia įrodinėti. Lietuvos bankas ginčo nagrinėjimo proceso metu neatlieka Lietuvos Respublikos Lietuvos banko įstatymo 42^1 straipsnyje reglamentuojamų patikrinimų, skirtų nustatyti ir įvertinti faktines aplinkybes dėl Lietuvos banko priežiūrimo finansų rinkos dalyvio galimo Lietuvos banko kompetencijai priskirtų teisės aktų reikalavimų pažeidimo. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Pareiškėjos ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjai banke atidarytoje pareiškėjos Sąskaitoje 2021 m. rugsėjo 8 d. atliktų Operacijų sumų – 7 700 Eur. Pareiškėja neigia autorizavusi Operacijas, taip pat mano, kad bankas nesiėmė visų veiksmų, kad būtų užtikrintas jos lėšų, esančių banko Sąskaitoje, saugumas. Bankas teigia, kad tretieji asmenys įgijo sąlygas inicijuoti Operacijas tik dėl to, kad pareiškėja dėl didelio neatsargumo sudarė visas sąlygas pasisavinti jos tapatybę ir jos vardu prisijungti bei inicijuoti Operacijas Sąskaitoje.

Siekiant išspręsti tarp pareiškėjos ir banko kilusį ginčą, Lietuvos banko vertinimu, būtina nustatyti šias pagrindines aplinkybes: 1) ar Operacijos laikytinos autorizuotomis, t. y. ar Operacijoms atlikti buvo gautas pareiškėjos sutikimas; 2) ar bankas turėjo (turi) pareigą grąžinti pareiškėjai Operacijų 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.

Dėl Operacijų autorizavimo

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

Mokėjimų įstatymo 37 straipsnio 1 dalyje nustatyta, kad tuo atveju, jeigu mokėtojas neigia autorizavęs įvykdytą mokėjimo operaciją ar teigia, kad mokėjimo operacija buvo įvykdyta netinkamai, jo mokėjimo paslaugų teikėjas turi įrodyti, kad mokėjimo operacijos autentiškumas buvo patvirtintas, ji buvo tinkamai užregistruota, įrašyta į sąskaitas ir jos nepaveikė techniniai trikdžiai arba kiti mokėjimo paslaugų teikėjo teikiamos paslaugos trūkumai; kai mokėtojas neigia autorizavęs įvykdytą mokėjimo operaciją, mokėtojo mokėjimo paslaugų teikėjo arba atitinkamais atvejais mokėjimo inicijavimo paslaugos teikėjo užregistruotas mokėjimo priemonės naudojimas nebūtinai yra pakankamas įrodymas, kad mokėtojas autorizavo mokėjimo operaciją ar veikė nesąžiningai arba tyčia ar dėl didelio neatsargumo neįvykdė vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų.

Pažymėtina, kad Mokėjimų įstatyme nėra nustatytų konkrečių mokėtojo sutikimo įvykdyti mokėjimo operaciją būdų ir (arba) išsamios 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).

Remiantis banko mokėjimo paslaugų teikimo sąlygų 3.3.1 papunkčiu, sutikimas dėl mokėjimo operacijos taip pat gali būti patvirtinamas tapatybės patvirtinimo priemonėmis. Visais šiame punkte numatytais būdais patvirtintas sutikimas laikomas kliento (mokėtojo) tinkamai patvirtintu, turinčiu tokią pačią teisinę galią kaip ir tokio kliento (jo atstovo) pasirašytas popierinis dokumentas (sutikimas), ir yra leistinas kaip įrodinėjimo priemonė, sprendžiant banko ir kliento ginčus teismuose bei kitose institucijose[2]. Ginčo šalių sudarytos elektroninių paslaugų teikimo sutarties[3] 6.8 papunktyje taip pat nurodyta, kad „naudotojo Tapatybės patvirtinimo priemonės ir jų pagalba išreikšta Naudotojo valia turi tokią pačią juridinę galią kaip ir Naudotojo, Sutartimi įgalioto Kliento atstovo, parašas ant rašytinio dokumento. Klientas ir/arba Naudotojas neturi teisės ginčyti Operacijos (pvz. mokėjimo nurodymo, sudarytos sutarties ir t.t.), jeigu Operaciją atliko Naudotojas, panaudodamas Tapatybės patvirtinimo priemones. Kliento vardu Elektroniniais kanalais su Banku sudarytos sutartys, patvirtintos/pasirašytos panaudojant Tapatybės patvirtinimo priemones, prilyginamos Kliento arba jo įgalioto asmens ir Banko raštu sudarytoms sutartims.“ Vadovaujantis elektroninių paslaugų teikimo sutarties 6.1 papunkčiu, „šalys susitaria, kad Operacijos gali būti tvirtinamos/pasirašomos: 6.1.1. elektroniniu parašu, kuris yra generuojamas panaudojant kodus nurodytus Banko išduotame identifikavimo kodų generatoriuje ar kitose Banko išduotose priemonėse, arba jų kombinacijas kaip nurodyta 6.1.4 p.; arba 6.1.2. Bankui priimtinu pažangiuoju elektroniniu parašu; arba 6.1.3. Bankui priimtinu kvalifikuotu elektroniniu parašu; arba 6.1.4. naudojant kitas Bankui priimtinas alternatyvias autorizavimo procedūras, kai Naudotojas savo valią išreiškia panaudodamas nuolatinį slaptažodį, slaptažodžius, SMS žinute siunčiamus kodus, unikalius mobilaus telefono aparato duomenis, mobilaus telefono numerį, išmaniajame įrenginyje nuskaitytus ir/ar išsaugotus biometrinius duomenis ir pan. arba šiame 6.1 punkte nurodytų būdų kombinacijomis.“

Pirmiau aptartose banko mokėjimo paslaugų teikimo sąlygų ir elektroninių paslaugų teikimo sutarties nuostatose kalbama apie atvejus, kai mokėtojas duoda savo sutikimą pervesti lėšas ir tuo tikslu panaudoja jam išduotas tapatybės patvirtinimo priemones (jų duomenis), tačiau nagrinėjamo ginčo atveju, priešingai, nei nurodyta minimose elektroninių paslaugų teikimo sutarties nuostatose, pareiškėja savo tapatybės patvirtinimo priemonę – „Smart-ID“ programėlę – panaudojo, taigi, PIN kodus joje suvedė, ne dėl to, kad ketino pervesti lėšas (atsiskaityti), o vykdydama, kaip pati tuo metu tikėjo, iš banko gautoje SMS žinutėje pateiktus nurodymus, skirtus pareiškėjos naudojamai tapatybės patvirtinimo priemonei „Smart-ID“ atnaujinti. Taigi, pareiškėja, tiek bendraudama su banku dėl Operacijų, tiek ir kreipimesi į Lietuvos banką nuosekliai laikosi pozicijos, kad valios inicijuoti Operacijas ir jas įvykdyti ji neišreiškė ir nedavė tam savo sutikimo – neautorizavo Operacijų šalių sutarta forma ir tvarka.

Bankas pateikė jo vidaus sistemose užfiksuotus duomenis, pagrindžiančius, kad Operacijos buvo autorizuotos, taikant saugesnio autentiškumo patvirtinimo procedūrą. Tačiau vien šie duomenys, Lietuvos banko vertinimu, dar neįrodo, kad Operacijos atliktos pareiškėjos sutikimu, t. y. kad mokėjimo nurodymai atlikti kredito pervedimus (Operacijas) iš tiesų atlikti pareiškėjos valia ir su jos 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, nelaikytina pakankamu įrodymu, jog mokėjimo priemone naudojosi ir (arba) mokėjimo operaciją autorizavo pats mokėtojas (Mokėjimų įstatymo 37 straipsnio 3 dalis).

Kaip matyti iš atsiliepime teikiamų paaiškinimų, bankas neneigia pareiškėjos nurodytos aplinkybės, kad Operacijos buvo patvirtintos ne pareiškėjos turimame ir jos naudojamame (valdomame) mobiliajame telefone su pačios pareiškėjos susikurta ir turima „Smart-ID“ tapatybės patvirtinimo priemone (t. y. pareiškėjos mobiliajame telefone esančia pareiškėjos vardu sukurta „Smart-ID“ Paskyra Nr. 1), o per trečiųjų asmenų valdomame mobiliajame įrenginyje pareiškėjos vardu susikurtą naują „Smart-ID“ paskyrą – Paskyrą Nr. 2 ir panaudojant

[2] Banko mokėjimo paslaugų teikimo sąlygų 2.1 papunktyje nurodyta, kad „Sąlygos taikomos visiems su Paslaugų teikimu susijusiems Kliento ir Banko santykiams, atsiradusiems iki ir tebesitęsiantiems po Sąlygų įsigaliojimo, bei atsiradusiems po Sąlygų įsigaliojimo“, o pagal 2.4 papunktį, „Sąlygos yra sudedamoji visų Sutarčių dalis. Sutarčių sudedamoji dalis taip pat yra Įkainiai ir atitinkamos Paslaugos sąlygos.“

[3] Nagrinėjamo ginčo kontekste aktuali elektroninių paslaugų teikimo sutarties bendrųjų sąlygų redakcija.

būtent šios paskyros slaptažodžius, sukurtus ir žinomus tretiesiems asmenims, kurie juos galėjo panaudoti inicijuodami ir patvirtindami Operacijas, pačiai pareiškėjai apie tai nežinant ir neišreiškus savo valios bei sutikimo dėl Operacijų. Taigi, bankas neginčija aplinkybės, kad pareiškėja neautorizavo Operacijų.

Sprendžiant Operacijų vertinimo kaip neautorizuotų klausimą, būtina pastebėti ir tai, kad, nors, vadovaujantis ginčo šalių sudarytos elektroninių paslaugų teikimo sutarties nuostatomis, pareiškėjai išduotos tapatybės patvirtinimo priemonės ir jas naudojant išreikšta valia prilyginama pareiškėjos parašui rašytiniuose dokumentuose, vis dėlto, nei ginčo šalių sudarytoje elektroninių paslaugų teikimo sutartyje, nei banko mokėjimo paslaugų teikimo sąlygose nėra paaiškinama, nurodoma „Smart-ID", kaip tapatybės patvirtinimo priemonės, PIN kodų suvedimo reikšmė mokėjimo operacijų vykdymo procese ir jų panaudojimo galimos pasekmės klientui. „Smart-ID" paskyros slaptažodžio PIN kodų suvedimo reikšmė mokėjimo operacijoms autorizuoti ir (ar) veiksmams su pačia „Smart-ID" paskyra atlikti kiek plačiau atskleidžiama tik banko interneto svetainėje esančioje „Smart-ID" atmintinėje[4].

Vadinasi, pagal abiejų ginčų šalių neginčijamas aplinkybes ir remiantis ginčo byloje turimais įrodymais – aplinkybe, kad Operacijų atlikimo dieną pareiškėjos vardu nauja „Smart-ID" paskyra buvo sukurta kitame mobiliajame įrenginyje, kuris nepriklauso pareiškėjai ir nėra jos naudojamas, ir, naudojantis šia paskyra – Paskyra Nr. 2 – pagal šalių neginčijamas aplinkybes buvo patvirtintos Operacijos, galima daryti prielaidą, kad Operacijos buvo inicijuotos ir patvirtintos ne pačios pareiškėjos, o trečiųjų asmenų, nors ir atitiko pareiškėjos ir banko sutartą sutikimo dėl mokėjimo operacijų davimo formą ir tvarką. Lietuvos banko nuomone, vertinti Operacijas kaip autorizuotas – atliktas esant pačios pareiškėjos sutikimui (kaip tai suprantama Mokėjimų įstatymo 29 straipsnio 1 dalies kontekste), nėra pagrindo, todėl šio ginčo nagrinėjimo metu Lietuvos bankas daro išvadą, kad Operacijos laikytinos neautorizuotomis.

Dėl neautorizuotų mokėjimo operacijų pasekmių ir pareiškėjos teisės į Operacijų sumos grąžinimą

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

Mokėjimų įstatymo 39 straipsnio 1 dalyje nustatyta, kad mokėtojas gali patirti dėl neautorizuotų mokėjimo operacijų atsiradusių nuostolių iki 50 Eur, 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 1) jis iki mokėjimo operacijos įvykdymo negalėjo pastebėti mokėjimo priemonės praradimo, vagystės arba neteisėto pasisavinimo, išskyrus atvejus, kai jis veikė nesąžiningai; 2) nuostoliai yra patirti dėl mokėjimo paslaugų teikėjo, jo darbuotojo, tarpininko, filialo ar asmenų, kuriems perduotas veiklos funkcijų valdymas, veiksmų ar neveikimo.

Remiantis Mokėjimų įstatymo 2 straipsnio 32 dalimi, „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.

Ginčo nagrinėjimo metu buvo nustatyta, kad, prieš inicijuojant ir įvykdant Operacijas, pareiškėja, vykdydama, kaip pati tuo metu tikėjo, iš banko gautoje SMS žinutėje pateiktus nurodymus, skirtus pareiškėjos naudojamai tapatybės patvirtinimo priemonei „Smart-ID" atnaujinti, paspaudė SMS pranešime pateiktą nuorodą ir suklastotame banko interneto puslapyje suvedė prašomus nurodyti asmens duomenis, o vėliau, aktyvavusis programėlei „Smart-ID", Paskyroje Nr. 1 suvedė šios paskyros PIN1 ir PIN2 kodus. Šie veiksmai, kaip matyti iš ginčo nagrinėjimo metu nustatytų aplinkybių, įgalino trečiuosius asmenis sukurti naują „Smart-ID" paskyrą kitame įrenginyje, kontroliuojamame trečiųjų asmenų, ir vėliau jų valiniais veiksmais pareiškėjos vardu inicijuoti ir patvirtinti Operacijas.

Kaip minėta, pareiškėja neigia autorizavusi Operacijas. Pareiškėjos teigimu, mokėjimo

[4] https://www.swedbank.lt/static/pdf/private/home/more/Smart_ID_atmintine_2019-11.pdf.

nurodymai įvykdyti Operacijas buvo pateikti vykdyti be jos žinios ir valinių veiksmų, t. y. pačiai pareiškėjai nedavus su banku sutarta forma ir tvarka sutikimo, kad būtų vykdomi tokie mokėjimo nurodymai. Ginčo nagrinėjimo metu padaryta išvada, kad Operacijos laikytinos neautorizuotomis. Bankas aplinkybės, kad Operacijos nebuvo pareiškėjos autorizuotos, taip pat neginčija ir, patvirtindamas pareiškėjos poziciją šiuo aspektu, nurodo, kad Operacijas galėjo inicijuoti ir patvirtinti ne pati pareiškėja, o tretieji asmenys, kurie neteisėtai išviliojo ir pasisavino pareiškėjos jiems per neatsargumą atskleistus (t. y. suklastotoje banko interneto svetainėje pareiškėjos suvestus) duomenis, būtinus prisijungti prie interneto banko sistemos, juos panaudojo naujai „Smart-ID" paskyrai sukurti trečiųjų asmenų kontroliuojamame įrenginyje ir tą pačią dieną, naudodamiesi nauja „Smart-ID" paskyra, inicijavo Operacijas. Taigi, įvertinus pareiškėjos ir banko pateiktą informaciją apie trečiųjų asmenų neteisėtus veiksmus, dėl kurių iš pareiškėjos Sąskaitos banke be jos valios buvo įvykdytos Operacijos, galima teigti, kad, atliekant šias Operacijas, pareiškėjos Sąskaita buvo neteisėtai užvaldyta trečiųjų asmenų.

Bankas savo sprendimą nekompensuoti pareiškėjos nuostolių, susijusių su Operacijų įvykdymu, grindžia tuo, kad, banko vertinimu, buvo nustatytos sąlygos vertinti pareiškėjos elgesį kaip labai neatsargų. Banko teigimu, tretieji asmenys galėjo inicijuoti Operacijas tik dėl to, kad pati pareiškėja dėl didelio neatsargumo sudarė visas sąlygas pasisavinti jos tapatybę ir jos vardu prisijungti prie pareiškėjos interneto banko paskyros ir inicijuoti Operacijas Sąskaitoje.

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 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 (Mokėjimų įstatymo 34 straipsnio 2 dalis).

Mokėjimų įstatymo 37 straipsnio 3 dalyje nustatyta, kad tuo atveju, kai mokėtojas neigia autorizavęs įvykdytą mokėjimo operaciją, mokėtojo mokėjimo paslaugų teikėjo arba atitinkamais atvejais mokėjimo inicijavimo paslaugos teikėjo užregistruotas mokėjimo priemonės naudojimas nebūtinai yra pakankamas įrodymas, kad mokėtojas autorizavo mokėjimo operaciją ar veikė nesąžiningai arba tyčia ar dėl didelio neatsargumo neįvykdė vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų. Mokėtojo mokėjimo paslaugų teikėjas ir atitinkamais atvejais mokėjimo inicijavimo paslaugos teikėjas turi pateikti įrodymų, kuriais patvirtinamas mokėtojo sukčiavimas arba didelis neatsargumas.

Įvertinus pirmiau nurodytas Mokėjimų įstatymo nuostatas, galima teigti, kad mokėtojo mokėjimo paslaugų teikėjas gali būti visiškai atleistas nuo pareigos grąžinti mokėtojui neautorizuotos mokėjimo operacijos sumą tik tuo atveju, jeigu pateikia įrodymų dėl mokėtojo sukčiavimo (nesąžiningumo arba tyčios) arba didelio neatsargumo (Mokėjimų įstatymo 37 straipsnio 3 dalis ir 39 straipsnio 3 dalis).

Pažymėtina, kad šalių ginčo dėl to, kad pareiškėja galėjo veikti nesąžiningai arba tyčia, įskaitant sukčiavimą, nėra. Tai reiškia, kad, siekiant įvertinti, ar šiuo atveju pareiškėjos atžvilgiu galėtų būti taikoma Mokėjimų įstatymo 39 straipsnio 3 dalis, būtina nustatyti, ar pareiškėjos elgesys, sudarant sąlygas tretiesiems asmenims neteisėtu būdu užvaldyti jos Sąskaitą, gali būti vertinamas kaip didelis pareiškėjos neatsargumas (aplaidumas), dėl kurio visi nuostoliai, susiję su Operacijų įvykdymu, turėtų tekti pareiškėjai.

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."

Pažymėtina, kad didelio neatsargumo sąvoka plėtojama ir 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.“[5]

Lietuvos banko nuomone, didelis neatsargumas ar paprastas neatsargumas yra vertinamojo pobūdžio aplinkybė ir išvada dėl mokėtojo elgesio vertinimo kaip neatsargaus ar labai neatsargaus dėl neautorizuotos (-ų) mokėjimo operacijos (-ų) ar dėl mokėjimo priemonės praradimo, lėmusio neautorizuotą (-as) mokėjimo operaciją (-as), darytina kiekvienu konkrečiu atveju, įvertinus ginčo nagrinėjimo metu 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 neautorizuotų mokėjimo operacijų įvykdymo ir su juo susijusių aplinkybių konteksto.

Lietuvos bankas, siekdamas nustatyti, ar pareiškėjos elgesys, įgalinant trečiuosius asmenis sukurti naują „Smart-ID“ paskyrą pareiškėjos vardu trečiųjų asmenų kontroliuojamame mobiliajame įrenginyje gali būti laikomas dideliu neatsargumu, vertino: pačios pareiškėjos elgesį tiek pasitikint SMS pranešime pateikta informacija apie būtinybę atnaujinti programėlės „Smart-ID“ duomenis ir spaudžiant joje pateiktą nuorodą, tiek suvedant savo mokėjimo priemonių personalizuotus saugumo duomenis suklastotame banko interneto banko puslapyje, tiek suvedant „Smart-ID“ Paskyros Nr. 1 PIN1 ir PIN2 slaptažodžius, aktyvavusis „Smart-ID“ programėlei, tiek ir banko veiksmus, kurių jis prevenciškai ėmėsi ir imasi tam, kad supažindintų pareiškėją su sukčiavimo elektroninėje erdvėje rizikomis bei tapatybės priemonės saugaus naudojimo, jos personalizuotų saugumo žymenų suvedimo ir atskleidimo reikšme bei teisinėmis pasekmėmis.

Vertinant pačios pareiškėjos elgesį, svarbu nustatyti, kaip pareiškėja, kaip mokėjimo paslaugų vartotoja, buvo įtikinta atskleisti savo mokėjimo priemonės personalizuotus saugos duomenis ir suvesti savo tapatybės patvirtinimo priemonės „Smart-ID“ PIN2 kodą, kuriuo buvo patvirtintas naujos „Smart-ID“ paskyros sukūrimas trečiųjų asmenų kontroliuojamame įrenginyje, iš kurio vėliau ir buvo įvykdytos abi neautorizuotos Operacijos.

Elektroninėje erdvėje nusikalstamas veikas vykdantys asmenys neretai pasitelkia įvairius būdus – tiek bendravimo, tiek klaidingos, suklastotos informacijos pateikimo, kad neteisėtu būdu įtikintų vartotoją atskleisti savo mokėjimo priemonių personalizuotus saugumo duomenis ir juos panaudodami įvykdytų (arba, kaip šiuo atveju, – sukurtų sąlygas įvykdyti) mokėjimo operacijas, kurių pats vartotojas neautorizuoja ir savo valinių veiksmų dėl tokių operacijų įvykdymo neišreiškia, kartais nežinodamas net apie tokių operacijų inicijavimo aplinkybę. Sprendžiant iš ginčo byloje esančių duomenų, pareiškėja į savo telefoną, į bendrą iš banko gautų žinučių srautą, gavo SMS pranešimą su „Swedbank“ logotipu ir inicialais. Pranešime buvo prašoma atnaujinti programėlės „Smart-ID“ duomenis, paspaudžiant ant pateiktos nuorodos. Paspaudusi pranešime pateiktą nuorodą, pareiškėja (šalių neginčijamomis aplinkybėmis) turėjo būti nukreipta į suklastotą banko interneto svetainę, kurioje pareiškėjai suvedus tam tikrus savo duomenis, jos naudojamos tapatybės patvirtinimo priemonės „Smart-ID“ Paskyra Nr. 1 aktyvavosi pareiškėjos telefone – tuomet pareiškėja, kaip matyti iš jos kreipimesi dėstomų aplinkybių, pasirodžius pranešimams, raginantiems suvesti šios paskyros PIN kodus, suvedė Paskyros Nr. 1 PIN1 slaptažodį ir po to iškart – PIN2 slaptažodį. Šie pareiškėjos veiksmai, kaip ir neteisėtu būdu pasisavinti pareiškėjos mokėjimo priemonių personalizuoti saugos duomenys, leido tretiesiems asmens sukurti naują „Smart-ID“ paskyrą pareiškėjos vardu ir ja naudojantis inicijuoti bei patvirtinti Operacijas. Papildomai pažymėtina, kad, nors pareiškėja kreipimesi teigia, kad SMS pranešimą, raginantį ją atnaujinti programėlės „Smart-ID“ duomenis, ji gavo tuo metu, kai buvo prisijungusi prie savo interneto banko ir tikrino, kiek pinigų buvo nurašyta iš jos Sąskaitos už degalinėje įsipiltus degalus, vis dėlto, remiantis banko pateiktais duomenis, paskutinė iki Operacijų įvykdymo pareiškėjos inicijuota prisijungimo prie interneto banko sesija prasidėjo 20:43:33 ir tęsėsi iki 20:45:37 val., o prašymą savo „Smart-ID“ Paskyroje Nr. 1 suvesti PIN1 slaptažodį pareiškėja gavo 21:20:26 val., t. y. praėjus daugiau nei pusvalandžiui nuo paskutinės prisijungimo prie interneto banko sesijos pabaigos.

Kaip minėta, bankas sprendimą nekompensuoti pareiškėjos nuostolių dėl Operacijų įvykdymo grindžia tuo, kad, jo vertinimu, sukčiai pareiškėjos Sąskaitą galėjo užvaldyti tik dėl

[5] Lietuvos Aukščiausiojo Teismo 2017 m. balandžio 13 d. nutartis civilinėje byloje Nr. e3K-3-180-378/2017, 29 punktas.

to, kad pareiškėjos elgesys buvo labai neatsargus. Bankas teigia, kad pareiškėja, gavusi banko vardu jai atsiųstą SMS pranešimą, kritiškai nevertino jo turinio ir besąlygiškai patikėjo pranešime nurodyta informacija tik dėl to, kad jame buvo naudojamas banko logotipas, kuriam suklastoti nereikia turėti jokių specialiųjų žinių. Bankas nurodo, kad pareiškėja suklastotoje banko interneto banko svetainėje, į kurią buvo nukreipta paspaudusi pranešime esančią aktyvią nuorodą, turėjo suvesti savo asmens kodą ir naudotojo ID, kitaip pareiškėjos ekrane nebūtų aktyvavęsis Paskyros Nr. 1 ekranas su prašymu suvesti PIN1 kodą. Atsižvelgdamas į šias aplinkybes, bankas mano, kad buvo nustatytos sąlygos pareiškėjos elgesį vertinti kaip labai neatsargų, nes pareiškėja tretiesiems asmenims atskleidė savo mokėjimo priemonių personalizuotus saugumo duomenis, taip pažeisdama savo, kaip mokėjimo paslaugų vartotojos, pareigas. Banko vertinimu, aplinkybė, kad pareiškėja neapsaugojo jai išduotų mokėjimo priemonių personalizuotų saugos duomenų konfidencialumo, kaip ir aplinkybė, kad pareiškėja, programėlėje „Smart-ID" gavusi pranešimus, raginančius ją suvesti jos naudojamos Paskyros Nr. 1 PIN kodus, neperskaitė veiksmų, kuriems duoda sutikimą suvesdama PIN kodus, aprašymo, rodo pareiškėjos didelį neatsargumą. Bankas taip pat mano, kad pareiškėjos didelis neatsargumas pasireiškė ir tuo, kad jai buvo būtina įsitikinti, ar per SMS atsiųstą nuorodą atsidaro tikras, o ne suklastotas banko svetainės puslapis, nes tai – viena iš esminių atidaus ir rūpestingo elgesio standartą atitinkančių saugaus elgesio internete, vykdant finansines operacijas, taisyklių.

Ginčo nagrinėjimo metu Lietuvos bankas paprašė pareiškėjos patikslinti, kokius duomenis ji suvedė suklastotoje banko interneto banko svetainėje, į kurią buvo nukreipta paspaudusi SMS parnešime pateiktą nuorodą. Pareiškėja nurodė, kad suklastotoje banko interneto banko svetainėje suvedė savo naudojo ID ir asmens kodą. Ši aplinkybė pagrindžia banko teiginį, kad, pareiškėjai neatskleidus interneto banko naudotojo ID ir savo asmens kodo, tretieji asmenys nebūtų galėję sukurti naujos „Smart-ID" paskyros pareiškėjos vardu. Tai reiškia, kad tretieji asmenys neteisėtu būdu sužinoję pareiškėjos dėl neatsargumo suklastotoje banko interneto banko aplinkoje suvestus personalizuotus saugumo duomenis, juos panaudojo Paskyrai Nr. 2 sukurti jau trečiųjų asmenų kontroliuojamame galiniame įrenginyje ir iš ten pareiškėjos vardu inicijavo bei patvirtino Operacijas savo naudai.

Vertinamų aplinkybių kontekste, vis dėlto, būtina pažymėti, kad remiantis pirmiau minėtų Mokėjimų įstatymo nuostatų analize, mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai tik tuo atveju, jei tenkinamos abi sąlygos. t. y. mokėtojas ne tik neįvykdo vienos ar kelių jam Mokėjimų įstatyme nustatytų pareigų, bet ir padaro tai elgdamasis nesąžiningai arba tyčia ar būdamas labai neatsargus. Taigi, banko sprendimas nekompensuoti pareiškėjos nuostolių dėl neautorizuotų Operacijų įvykdymo galėtų būti vertinamas kaip pagrįstas tik tuo atveju, jei būtų įrodyta, kad pareiškėja, sudarydama sąlygas tretiesiems asmenims užvaldyti jos Sąskaitą ir tokiu būdu įvykdyti pačias Operacijas, elgėsi itin aplaidžiai – buvo labai neatsargi.

Nors bankas atsiliepime teigia, kad pareiškėja, banko vardu gavusi SMS pranešimą apie būtinybę atnaujinti „Smart-ID" programėlę, turėjo kritiškai vertinti jos turinį, nes, norint suklastoti tokį pranešimą, kaip ir jame galimai pateiktą banko logotipą, nereikia jokių specialiųjų žinių, vis dėlto abejotina, ar vidutiniam vartotojui vien tokia aplinkybė neabejotinai turėjo būti savaime ir iškart suprantama, todėl manytina, kad aplinkybės, jog aptariamas trečiųjų asmenų (sukčių) atsiųstas SMS pranešimas buvo gautas ir pateko į bendrą kitų iš banko gautų žinučių srautą, o jame buvo naudojamas banko logotipas, galėjo sukurti įspūdį, kad ši žinutė buvo iš tiesų atsiųsta banko, ir pareiškėjai nesant itin aplaidžiai. Be to, nors atsiliepime bankas nurodo, kad nėra matęs pareiškėjos gauto SMS pranešimo, tačiau kartu teigia, kad jame banko pavadinimas nurodytas klaidingas. Vis dėlto, remiantis pareiškėjos kartu su papildomais paaiškinimais pateiktu jos mobiliojo telefono ekrano vaizdu, kuriame matyti iš trečiųjų asmenų gautas SMS pranešimas, raginantis pareiškėją atnaujinti „Smart-ID" programėlę, banko pavadinimas yra nurodytas teisingai – „Swedbank".

Bankas taip pat teigia, kad pareiškėjos labai neatsargus elgesys pasireiškė tuo, kad ji neįsitikino, ar interneto svetainė, į kurią ji buvo nukreipta paspaudusi SMS pranešime pateiktą nuorodą, iš tiesų yra banko interneto svetainė, o ne suklastotas puslapis, kuriame pareiškėja suvedė ir tretiesiems asmenims atskleidė savo personalizuotus saugos duomenis, įgalinusius trečiuosius asmenis sukurti naują „Smart-ID" paskyrą. Vis dėlto atkreiptinas dėmesys, kad ginčo byloje nėra duomenų – jų (tokios interneto svetainės ekrano vaizdų) kartu su kreipimusi ir atsiliepimu nepateikė nei pareiškėja, nei bankas – kaip atrodė suklastotas banko interneto puslapis, į kurį buvo nukreipta pareiškėja, kaip ir kokių duomenų (be pareiškėjos ir banko

nurodytų) jame pareiškėjos buvo prašoma suvesti. Taigi, negalima pagrįstai teigti, kad pareiškėja itin neapdairiai pasitikėjo interneto puslapiu ir jame nurodyta informacija, kuris vidutiniam vartotojui turėjo neabejotinai kelti rimtų įtarimų bei abejonių ir atrodyti akivaizdžiai suklastotas, todėl turėjo kilti poreikis ir vidutinis vartotojas žinotų, kaip patikrinti interneto svetainės autentiškumą. Vadinasi, savaime vertinti vien dėl šios aplinkybės pareiškėjos elgesio kaip itin aplaidaus nėra pagrindo – įrodymų.

Kita vertus, neabejotina, kad vartotojai, naudodamiesi mokėjimo paslaugomis elektroninėje erdvėje, taip pat privalo paisyti saugaus elgesio rekomendacijų, ir, pagrįstai tikėdamiesi aukštus profesionalumo, rūpestingumo ir atidumo standartus atitinkančio mokėjimo paslaugų teikėjo elgesio, patys būti apdairūs, atidūs ir sąmoningi, nes vartotojų lėšų ir atliekamų mokėjimo operacijų, kaip ir kitų elektroninėje erdvėje teikiamų mokėjimo paslaugų, saugumas priklauso ir nuo tinkamo bei atidaus mokėjimo paslaugų vartotojo pareigų, susijusių su mokėjimo priemonių naudojimu, vykdymo.

Ginčo byloje esantys duomenys neleidžia vertinti pareiškėjo elgesio kaip atitinkančio banko viešai skelbiamas saugaus naudojimosi elektroninėmis paslaugomis rekomendacijas: nors, kaip minėta, aplinkybės, kad trečiųjų asmenų siųstas SMS pranešimas pateko į bendrą kitų iš banko gautų žinučių srautą, o jame buvo panaudotas banko logotipas, galėjo sukurti pirminį įspūdį, kad šis pranešimas siųstas banko, vis dėlto tai, kad pareiškėja nesudvejojo SMS pranešime nurodytos informacijos patikimumu, nors minėtas SMS pranešimas, kaip matyti iš pareiškėjos pateiktų jos mobiliojo telefono ekrano vaizdų, buvo parašytas be lietuviškų rašmenų, (o tokių pranešimų bankas nesiunčia) neleidžia vertinti pareiškėjos elgesio kaip pakankamai atidaus ir rūpestingo. Pareiškėja taip pat nekvestionavo pagal pranešime paspaustą nuorodą atsidariusio interneto puslapio autentiškumo, o jei tokių abejonių pareiškėja turėjo, ginčo byloje nėra jokių duomenų, kad šias abejones būtų stengusis išsklaidyti, patikrinti gautos informacijos teisingumą. Priešingai, ginčo nagrinėjimo metu nustatytomis bei pačios pareiškėjos nurodytomis aplinkybėmis pareiškėja nedvejodama paspaudė gautame SMS pranešime pateiktą nuorodą ir atsidariusiame interneto puslapyje iškart suvedė prašomus nurodyti savo naudotojo ID ir asmens kodą, o vėliau, nedelsdama ir nedvejodama suvedė savo naudojamos „Smart-ID" Paskyros Nr. 1 PIN1 ir PIN2 kodus. Nepaisant to, kad, kaip buvo minėta pirmiau, banko ir pareiškėjos sudarytoje elektroninių paslaugų teikimo sutartyje ir mokėjimo paslaugų teikimo sąlygose tapatybės patvirtinimo priemonės „Smart-ID" tiek PIN2 kodo, tiek apskritai PIN kodų suvedimas ir jų reikšmė mokėjimo operacijoms autorizuoti bei naudotis kitomis banko paslaugomis nėra atskirai detalizuojami, tačiau, manytina, pareiškėjai, kuri turi naudojimosi šia tapatybės patvirtinimo priemone patirties, turėjo sukelti įtarimų vien faktas, kad jos buvo prašoma atnaujinti „Smart-ID" programėlės duomenis, spaudžiant SMS pranešime pateiktą nuorodą, ir turėjo būti žinoma, kad, prieš suvedant programėlės „Smart-ID" atsiradusiuose pranešimuose PIN kodus, pareiškėja turi su pranešimais susipažinti ir aktyviais veiksmais patvirtinti, kad supranta, kokius veiksmus atlieka, ir savo valią dėl jų išreikšti PIN kodų suvedimu.

Atsiliepime bankas, be kita ko, nurodo, kad „Smart-ID" nėra banko sukurta tapatybės patvirtinimo priemonė ir bankas tik suteikia galimybę klientams naudotis ja autentifikavimosi tikslais. Vis dėlto pažymėtina, kad, nors „Smart-ID" ir nėra banko sukurta tapatybės patvirtinimo priemonė, būtent bankas suteikia galimybę naudojantis ja savo klientams (šiuo atveju – pareiškėjai) nuotoliniu būdu patvirtinti savo tapatybę ir išreikšti savo valią atlikti tam tikrus veiksmus, sukeliančius jiems teisines pasekmes – t. y. naudotis banko teikiamomis paslaugomis – pateikti mokėjimo nurodymą, pasitikrinti sąskaitą ir pan. Tad banko siūlomos ir (ar) leidžiamos naudoti tapatybės patvirtinimo priemonės ne tik turi būti saugios klientams, kurie su banku susiklosčiusiuose sutartiniuose santykiuose naudoja atitinkamą tapatybės patvirtinimo priemonę, bet ir turi būti aiškios: aiškiai pateiktos jos naudojimo sąlygos ir veiksmų, atliekamų su „Smart-ID", teisinės pasekmės – pavyzdžiui, aiški PIN kodų suvedimo teisinė reikšmė.

Vertinant pareiškėjos elgesį ir atsakomybės laipsnį dėl Sąskaitos užvaldymo ir neautorizuotų operacijų įvykdymo, atsižvelgtina ir į tai, kad, kaip minėta pirmiau, nei ginčo šalių sudarytoje elektroninių paslaugų teikimo sutartyje, nei banko mokėjimo paslaugų teikimo sąlygose nėra paaiškinama, nurodoma, kokia yra šios tapatybės patvirtinimo priemonės PIN kodų suvedimo reikšmė mokėjimo operacijų vykdymo procese ir kokios galimos panaudojimo pasekmės klientui, t. y. kokius veiksmus, naudodamasis „Smart-ID" programėle, banko klientas gali atlikti, ir kokie veiksmai, naudojantis šia tapatybės patvirtinimo priemone, sukelia atitinkamas teisines pasekmes. „Smart-ID" paskyros PIN kodų suvedimo reikšmė mokėjimo

operacijoms autorizuoti ir (ar) veiksmams su pačia „Smart-ID" paskyra atlikti kiek plačiau atskleidžiama tik banko interneto svetainėje esančioje „Smart-ID" atmintinėje. Kita vertus, kaip nurodo bankas atsiliepime, pateikdamas tai pagrindžiančius įrodymus, pareiškėja iki Paskyros Nr. 2 sukūrimo ne kartą nuotoliniu būdu yra davusi sutikimą sukurti naują „Smart-ID" paskyrą jos vardu: iki Paskyros Nr. 2 sukūrimo 2021 m. rugsėjo 8 d. pareiškėjos vardu buvo sukurtos 6 „Smart-ID" paskyros, tik 2 iš jų buvo sukurtos jai fiziškai dalyvaujant banko klientų aptarnavimo padalinyje. Minėta aplinkybė leidžia pagrįstai teigti, kad šiuo konkrečiu atveju pareiškėjai turėjo būti žinoma, kad naudojantis jos turima tapatybės patvirtinimo priemone – Paskyra Nr. 1, galima ne tik inicijuoti ir patvirtinti mokėjimo nurodymus, inicijuoti sutarčių, sudarytų su banku, pakeitimus ir pan., bet ir atlikti veiksmus su pačia tapatybės patvirtinimo priemone – pavyzdžiui, sukurti naują „Smart-ID" paskyrą kitame galiniame įrenginyje.

Vystantis ir tobulėjant technologijoms, vystomi ir sukčiavimo būdai bei priemonės, sudėtingėja pačios sukčiavimo atakos, todėl jas atpažinti ir nuo jų apsisaugoti reikia vis didesnio mokėjimo paslaugų vartotojų atidumo ir rūpestingumo. Taigi, dėl naujų sukčiavimo būdų, panaudojant naujas technologijas, atsiradimo būtinas itin aukštas vartotojų pastabumas ir apdairumas, kuris kartais dėl sukčiavimo atakos naujumo ir kompleksiškumo peržengia net ir vidutinio vartotojo gebėjimą laiku identifikuoti mėginimą neteisėtu būdu pasisavinti mokėjimo priemonę ir (ar) įvykdyti mokėjimo operacijas, kurių mokėjimo paslaugų vartotojas nesiekia įvykdyti. Dėl šios priežasties manytina, kad mokėjimo paslaugų teikėjai, kaip savo srities profesionalai, turi dėti reikiamas pastangas, kad nuolat kryptingai ir tinkamai informuotų savo klientus (vartotojus) apie sukčiavimo pavojus ir rizikas, susijusias su sukčiavimais elektroninėje erdvėje, ir primintų, kokie ir kaip vartotojų duomenys turėtų būti saugomi ir neatskleisti tretiesiems asmenims.

Bankas atsiliepime nurodo, kad, siekdamas tinkamai informuoti mokėjimo paslaugų vartotojus apie kylančias rizikas naudojantis mokėjimo paslaugomis elektroninėje erdvėje, nuolat įvairiais būdais perspėja savo klientus apie sukčiavimo atakas ir ragina juos būti labai atidžius, niekada neatskleisti, nevesti savo asmens, mokėjimo kortelių ir interneto banko prisijungimo duomenų trečiųjų asmenų prašymu, kritiškai tokius prašymus įvertinti[6]. Bankas nurodė, kad 2021 m. rugsėjo 8 d. banko interneto puslapyje paskelbė pranešimą, aiškiai matomą klientams jungiantis prie interneto banko: „Būkite atsargūs! Pastaruoju metu gyventojai sulaukia skambučių bei SMS žinučių su nuorodomis į netikrą „Swedbank" puslapį, skatinant atblokuoti užblokuotas sąskaitas ar sustabdyti neegzistuojančius pavedimus. Prašome nespausti nuorodų žinutėse ir netvirtinti jokių operacijų, kurių patys neinicijavote. Primename, kad bankas niekada nesiunčia SMS žinučių su nuorodomis ir neprašo atskleisti prisijungimo duomenų, slaptažodžių, PIN kodų ar kitos asmeninės informacijos. Taip pat banko darbuotojai jokiais atvejais nevyksta suteikti paslaugų į namus." Be šios informacijos, kartu nurodoma, kad „saugokite savo prisijungimo priemones: kodus įsiminkite, o ne užsirašykite, niekam jų neatskleiskite, apsaugokite savo išmaniuosius įrenginius ekrano užraktu. Jei praradote prisijungimo priemonę ar išmanųjį telefoną arba pastebėjote įtartinas operacijas savo banko sąskaitoje, nedelsdami praneškite mums tel. 1884. Peržvelkite kitas saugaus naudojimosi banko e-paslaugomis rekomendacijas." Bankas atsiliepime taip pat informavo, kad 2021 m. liepos 15 d. naktį banko mobiliosios programėlės naudotojams buvo pradėtas rodyti tekstas, kurį matė visi šios programėlės naudotojai, pradėję naudotis banko išmaniąja programėle nuo nurodytos datos: „Būkite atsargūs! Sukčiai neatostogauja. Jie nuolat kuria naujus būdus, kaip pasisavinti jūsų duomenis. Tai gali būti SMS su netikromis nuorodomis, skambučiai, e. laiškai ir žinutės jūsų socialiniuose tinkluose. Niekuomet neįveskite savo PIN kodų, jei neinicijavote bankinės operacijos patys." Norėdami pradėti naudotis išmaniąja programėle, klientai, taigi, ir pareiškėja, turėjo paspausti, kad susipažino su pranešimu. Bankas papildomai nurodė, kad kartą per metus taip pat informuoja savo klientus apie saugaus naudojimosi elektroninėmis paslaugomis rekomendacijas. Banko pateiktais duomenimis, 2020 m. kovo 30 d. pareiškėjai interneto banko žinute buvo išsiųstas toks pranešimas, tačiau ji pasirinko šio pranešimo neskaityti. Nurodytos aplinkybės leidžia teigti, kad bankas, kaip mokėjimo paslaugų srities profesionalas, deda pakankamai daug pastangų, kad informuotų mokėjimo paslaugomis besinaudojančius savo klientus, tarp jų ir pareiškėją, apie elektroninėje erdvėje kylančias rizikas.

Sprendžiant dėl pareiškėjos reikalavimo pagrįstumo, įvertintina ir tai, kad trečiųjų asmenų įvykdyta sukčiavimo ataka buvo sofistikuota – įvykdyta pasinaudojant egzistuojančia

[6] Banko interneto puslapyje viešai skelbiamos saugaus naudojimosi elektroninėmis paslaugomis rekomendacijos, https://www.swedbank.lt/private/d2d/ebanking/secureBanking?language=LIT.

technine galimybe sukurti naują tapatybės patvirtinimo priemonės „Smart-ID" paskyrą nuotoliniu būdu kitame mobiliajame įrenginyje. Iš ginčo nagrinėjimo metu nustatytų aplinkybių matyti, kad tretieji asmenys pasitelkė priemones, kad sukurtų įspūdį, jog pareiškėja, naudodamasi savo tapatybės patvirtinimo priemone, atlieka veiksmus ir vykdo banko nurodymus banko internetinėje aplinkoje, kurioje, pasitikėdama nurodyta informacija, pareiškėja ir atskleidė savo personalizuotus saugos duomenis, suvesdama interneto banko naudotojo atpažinimo kodą ir savo asmens kodą, o vėliau, atsiradus atitinkamiems pranešimams, suvedė ir savo „Smart-ID" Paskyros Nr. 1 PIN1 ir PIN2 kodus. Ginčo nagrinėjimo metu nustatyta, kad „Smart-ID" Paskyros Nr. 1 PIN2 kodo suvedimu buvo patvirtinta naujos „Smart-ID" paskyros sukūrimas – Paskyra Nr. 2, ir šia paskyra naudojantis, pačiai pareiškėjai nedalyvaujant, t. y. pačiai pareiškėjai neinicijuojant ir nepatvirtinant (neautorizuojant), ir neišreiškiant jokių kitų valios veiksmų, buvo įvykdytos Operacijos, apie jų inicijavimo ir įvykdymo faktą pareiškėjai nežinant iki atitinkamo banko pranešimo, kad Operacijos buvo įvykdytos.

Ginčo nagrinėjimo metu Lietuvos bankas taip pat paprašė banko pateikti papildomus paaiškinimus ir juos pagrindžiančius duomenis, ar, tretiesiems asmenims tvirtinant abi Operacijas iš pareiškėjos vardu sukurtos naujos „Smart-ID" paskyros trečiųjų asmenų kontroliuojamame mobiliajame įrenginyje, pareiškėjos telefone taip pat atsirado („iššoko") pačios pareiškėjos naudojamos tapatybės patvirtinimo priemonės „Smart-ID" Paskyros Nr. 1 pranešimai, prašantys suvesti PIN1 kodą, kad būtų prisijungta prie interneto banko paskyros, ir PIN2 kodą, kad būtų patvirtinta atitinkama mokėjimo operacija. Bankas, paaiškindamas prašomas aplinkybes ir remdamasis iš „SK ID Solutions AS" gautais paaiškinimais, nurodė, kad, jei kliento vardu yra įdiegta „Smart-ID" programėlė keliuose įrenginiuose, užklausos dėl sutikimo davimo siunčiamos į visus įrenginius vienu metu. Taigi, banko teigimu, pranešimai, prašantys patvirtinti pareiškėjos prisijungimą prie interneto banko, ir pranešimai, prašantys patvirtinti Operacijas, turėjo pasirodyti abiejuose įrenginiuose, su kuriais buvo susietos pareiškėjos vardu sukurtos „Smart-ID" paskyros. Bankas, vadovaudamasis prisijungimo prie banko interneto banko Operacijų įvykdymo dieną vidinės sistemos duomenimis, nurodo, kad tą aplinkybę, jog prašymai duoti sutikimą dėl Operacijų buvo siunčiami tiek į pareiškėjos įrenginį, kuriame įdiegta Paskyra Nr. 1, tiek ir į trečiųjų asmenų valdomą įrenginį, kuriame įdiegta Paskyra Nr. 2, patvirtina tas faktas, kad jau po Paskyros Nr. 2 sukūrimo, 21:24:43 val., bet dar iki Operacijų inicijavimo (informacija apie duotus sutikimus dėl Operacijų bankas gavo 21:27:30 val. ir 21:28:59 val.) buvo inicijuotas prisijungimas pareiškėjos vardu prie trečiųjų asmenų įrenginyje įdiegtos „Swedbank" išmaniosios programėlės, o sutikimas jam duotas pareiškėjos Paskyrai Nr. 1 taikomu PIN1 slaptažodžiu: taigi, užklausos buvo parodytos abiejuose įrenginiuose, o pareiškėja pirmiau už Paskyros Nr. 2 valdytojus davė sutikimą prisijungti prie „Swedbank" išmaniosios programėlės.

Vis dėlto, įvertinus pirmiau aptartą informaciją, būtina pažymėti, kad banko papildomai pateikti duomenys nepagrindžia aplinkybės, kad pareiškėja tikrai matė, jog jos vardu Sąskaitoje buvo siekiama įvykdyti būtent Operacijas. T. y. ginčo byloje nėra jokių duomenų, kad pareiškėjos telefone pagrindiniame ekrane turėjusius automatiškai pasirodyti („iššokti") pranešimus ir tai, koks buvo šių pranešimų turinys, pareiškėja tikrai matė, nes tokios aplinkybės pati pareiškėja nepatvirtina. Priešingai, ginčo nagrinėjimo metu pareiškėjos paprašius pateikti paaiškinimus dėl šios banko nurodytos aplinkybės – t. y. kad pranešimai, prašantys patvirtinti Operacijas, turėjo pasirodyti pareiškėjos telefone, aktyvavusis jos naudojamai „Smart-ID" Paskyrai Nr. 1, pareiškėja nurodė, kad tokie pranešimai jos telefone nepasirodė, o apie Operacijų įvykdymo faktą ji sužinojo tik gavusi žinutes apie lėšų pervedimus gavėjui Y. Y. ir prisijungusi prie banko mobiliosios programėlės. Būtina pažymėti, kad papildomuose paaiškinimuose bankas nurodė, pateikdamas tai patvirtinančius įrodymus, kad abi pareiškėjos ginčijamos Operacijos buvo tiek inicijuotos, tiek patvirtintos iš trečiųjų asmenų galinio įrenginio, naudojantis trečiųjų asmenų sukurta Paskyra Nr. 2 ir suvedant šios paskyros PIN kodus. Ginčo byloje nėra jokių duomenų, kiek laiko atsiradęs pranešimas (jei toks turėjo atsirasti), prašantis suvesti PIN1 ir PIN2 kodus, galėjo būti rodomas pareiškėjos telefone – turėtina omenyje ir tai, kad abi Operacijos buvo patvirtintos iš trečiųjų asmenų kontroliuojamos pareiškėjos vardu sukurtos naujos „Smart-ID" paskyros ir šios paskyros PIN kodai, susidedantys iš 4–5 skaitmenų, tikėtina, buvo suvesti per sekundę, daugiausia – per kelias sekundes. Be to, nėra ir jokių duomenų, kad pareiškėja būtent Operacijų įvykdymo metu telefoną turėjo šalia savęs ir turėjo galimybę pranešimus pamatyti.

Pareiškėja, pagrįsdama banko atžvilgiu keliamą reikalavimą dėl nuostolių, susijusių su

Operacijų įvykdymu, kompensavimo, be kita ko, teigia, kad bankas nesiėmė visų veiksmų, kad būtų užtikrintas jos lėšų, esančių banko Sąskaitoje, saugumas. Taigi, pareiškėja preziumuoja, kad banko pritaikytos saugumo priemonės (operacijų stebėjimo mechanizmai) buvo nepakankamos, o tai patvirtina faktas, kad bankas neautorizuotų mokėjimo operacijų sumas pervedė sukčiams.

2017 m. lapkričio 27 d. Komisijos deleguotojo reglamento (ES) 2018/389, kuriuo Europos Parlamento ir Tarybos direktyva (ES) 2015/2366 papildoma griežto kliento autentiškumo patvirtinimo ir bendrų ir saugių atviruųjų ryšių standartų techniniais reguliavimo standartais (toliau – Reglamentas)[7] ir kuris priimtas siekiant užtikrinti, kad elektroniniu būdu siūlomos mokėjimo paslaugos būtų teikiamos saugiai, įdiegiant technologijas, kuriomis galima užtikrinti saugų vartotojo autentiškumo patvirtinimą ir kuo labiau sumažinti sukčiavimo riziką, 2 straipsnyje nustatyti bendrieji autentiškumo patvirtinimo reikalavimai, kurių tinkamą įvykdymą turi užtikrinti mokėjimo paslaugų teikėjai. Pagal minėto straipsnio nuostatas, mokėjimo paslaugų teikėjai įdiegia operacijų stebėjimo mechanizmus, leidžiančius jiems aptikti neautorizuotas ar nesąžiningas mokėjimo operacijas, kad galėtų įgyvendinti saugumo priemones, nurodytas Reglamento 1 straipsnio a ir b punktuose. Tie mechanizmai yra grindžiami mokėjimo operacijų analize, kurią atliekant atsižvelgiama į mokėjimo paslaugų vartotojui būdingus elementus įprastu būdu naudojant personalizuotus saugumo požymius (1 dalis). Mokėjimo paslaugų teikėjai užtikrina, kad operacijų stebėjimo mechanizmais būtų atsižvelgiama į kiekvieną iš šių rizika grindžiamų veiksnių: a) neteisėtai sužinotų ar pavogtų autentiškumo nustatymo elementų sąrašus; b) kiekvienos mokėjimo operacijos sumą; c) žinomus sukčiavimo scenarijus teikiant mokėjimo paslaugas; d) užkrėtimo kenkimo programine įranga požymius per bet kurį autentiškumo patvirtinimo procedūros seansą; e) tais atvejais, kai prieigos prietaisą arba programinę įrangą suteikė mokėjimo paslaugų teikėjas, mokėjimo paslaugų vartotojui suteikto prieigos prietaiso arba programinės įrangos naudojimo ir netinkamo jų naudojimo žurnalą. Be to, remiantis Reglamento nuostatomis, autentiškumo patvirtinimo procedūra turėtų apimti operacijų stebėjimo mechanizmus, kuriais būtų galima nustatyti mėginimus pasinaudoti mokėjimo paslaugų vartotojo personalizuotais saugumo požymiais, kurie buvo prarasti, pavogti arba neteisėtai pasisavinti, ir užtikrinti, kad mokėjimo paslaugų vartotojas, įprastu būdu nurodęs personalizuotus saugumo požymius, būtų teisėtas vartotojas ir kaip toks išreikštų savo sutikimą pervesti lėšas ir gauti informaciją apie savo sąskaitą[8].

Atsižvelgdamas į pareiškėjos išreikštas abejones dėl taikomų saugumo priemonių pakankamumo, bankas atsiliepime nurodė, kad yra įgyvendinęs ir taikė Operacijoms griežto kliento autentiškumo patvirtinimo saugumo priemones. Be to, banko vertinimu, Operacijos neatitiko kriterijų, dėl kurių galėtų būti stabdomos mokėjimo operacijos, vykdant pinigų plovimo ir teroristų finansavimo prevencijos reikalavimus – bankas nurodo, kad vien ta aplinkybė, kad lėšos konkrečiam gavėjui buvo pervestos pirmąkart, nedaro atitinkamos operacijos įtartina. Bankas nurodo neturėjęs jokio pagrindo (teisėtų priežasčių) nevykdyti Operacijų, nes sutikimo Operacijoms davimo metu pareiškėjos tapatybė buvo patvirtinta taikant sustiprintą tapatybės nustatymo procedūrą, o Operacijų įvykdymo metu jokių sutrikimų banko informacinėje sistemoje nebuvo fiksuota.

Bankas Lietuvos bankui nepateikė duomenų, ar, vykdant Operacijas, banke buvo įdiegti ir taikomi mokėjimo operacijų stebėjimo mechanizmai, vykdyta pareiškėjos vardu inicijuotų mokėjimo nurodymų įvykdyti Operacijas analizė, taikytos kitos priemonės, kad pareiškėjos vardu iš jos Sąskaitos nebūtų įvykdytos pačios pareiškėjos neautorizuotos mokėjimo operacijos. Kaip matyti iš banko pateiktų paaiškinimų, bankas, siekdamas įgyvendinti Reglamento ir Mokėjimų įstatymo reikalavimus, susijusius su saugumo priemonių įgyvendinimu, taiko griežto kliento autentiškumo patvirtinimo saugumo priemones, t. y. bankas klientų inicijuotoms mokėjimo operacijoms autorizuoti taiko saugesnio autentiškumo nustatymo procedūrą. Lietuvos bankas neturi pakankamai duomenų, kad galėtų patvirtinti ar paneigti aplinkybę, jog bankas nagrinėjamu atveju ėmėsi pakankamų saugumo priemonių, vykdydamas Operacijas, kaip tai nustatyta Reglamento nuostatose, tačiau faktas, kad visos Operacijos buvo patvirtintos taikant saugesnio autentiškumo patvirtinimo procedūrą, įrodytas. Kaip minėta, Lietuvos bankas ginčo nagrinėjimo metu neatlieka patikrinimų, kad nustatytų, ar nebuvo pažeisti teisės aktų reikalavimai. Lietuvos bankas remiasi ginčo šalių pateiktais konkrečiais įrodymais, kurių pagrindu priima sprendimą. Nors pareiškėja kreipimesi teigia, kad banko pritaikytos saugumo

[7] https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32018R0389&from=EN.
[8] Reglamento preambulės 1 punktas.

priemonės (operacijų stebėjimo mechanizmai) šiuo atveju buvo nepakankamos, tačiau savo teiginį patvirtinančių įrodymų nepateikė. Taigi, ginčo byloje nėra duomenų, kurių pagrindu būtų galima vertinti, ar bankas, įvykdydamas Operacijas, pažeidė finansų rinką reglamentuojančių teisės aktų reikalavimus.

Kita vertus, aplinkybė, kad Operacijos buvo patvirtintos naudojant mokėjimo operacijoms autorizuoti šalių sutartiniuose santykiuose sutartus naudoti saugesnio autentiškumo nustatymo reikalavimus, šiuo atveju, esant įrodymų, kad šalių sutarta mokėjimo operacijų saugesnio autentiškumo patvirtinimo procedūra tretieji asmenys pasinaudojo be pareiškėjos žinios ir valios veiksmų bei sutikimo, nedaro tokių operacijų autorizuotomis, bet kartu, kaip buvo konstatuota pirmiau, ir savaime nesuponuoja išvados, kad pareiškėjos elgesys, įgalinant trečiuosius asmenis sukurti naują „Smart-ID" paskyrą ir užvaldyti jos Sąskaitą, vertintinas kaip labai neatsargus.

Lietuvos banko nuomone, mokėtojo 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. Kaip jau buvo minėta pirmiau, Mokėjimų įstatymo 34 straipsnyje reglamentuojama viena iš mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigų – naudotis mokėjimo priemone pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas. Banko mokėjimo paslaugų teikimo sąlygų 7.1 papunktyje, reglamentuojančiame su mokėjimo priemone susijusias banko kliento pareigas, nustatyta, kad: „7.1.1. Klientas, turintis teisę naudotis Mokėjimo priemone, privalo: 7.1.1.1. naudotis Mokėjimo priemone pagal Mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, nurodytas atitinkamoje Sutartyje ir/ar Paslaugos sąlygose; 7.1.1.2. sužinojęs apie Mokėjimo priemonės vagystę ar praradimą kitu būdu, įtarus ar sužinojus apie Mokėjimo priemonės neteisėtą įgijimą arba neautorizuotą jos naudojimą, taip pat apie faktus ar įtarimus, kad Mokėjimo priemonės personalizuotus saugumo duomenis (įskaitant Tapatybės patvirtinimo priemones) sužinojo arba jais gali pasinaudoti Tretieji asmenys, nedelsdamas apie tai pranešti Bankui ar kitam jo nurodytam subjektui, vadovaujantis Mokėjimo priemonės išdavimą ir naudojimą reglamentuojančiomis sąlygomis, nurodytomis Sutartyje ir/ar Paslaugos sąlygose. 7.1.2. Klientas, gavęs Mokėjimo priemonę, privalo iš karto imtis visų veiksmų (įskaitant nurodytus Paslaugos sąlygose ir atitinkamoje Sutartyje), kad būtų apsaugoti gautos Mokėjimo priemonės personalizuoti saugumo duomenys (įskaitant Tapatybės patvirtinimo priemones)." Be to, vadovaujantis banko viešai skelbiamomis saugaus naudojimosi elektroninėmis paslaugomis rekomendacijomis, banko klientai raginami nespausti jokių el. paštu, pokalbių programėlėse ar SMS žinutėse gautų nuorodų, nevykdyti prašymų suvesti arba padiktuoti prisijungimo prie interneto banko ar kortelės duomenis, atidžiai įvertinti savo telefono ekrane matomą prašymą įvesti turimos prisijungimo priemonės slaptažodį, jei nėra su kuo sulyginti kontrolinio kodo arba jis nesutampa, arba ignoruoti tokį pranešimą, jei nesiekiama prisijungti prie interneto banko ar inicijuoti mokėjimo operacijų, kilus nors mažiausiai abejonei, neskubėti ir nedelsiant nutraukti veiksmus[9].

Iš pirmiau aptartų banko mokėjimo paslaugų teikimo sąlygų nuostatų matyti, kad jose aiškiai ir nedviprasmiškai reglamentuojama, kad už tapatybės priemonės personalizuotų saugumo duomenų konfidencialumą yra atsakingas mokėtojas, šiuo atveju – pareiškėja.

Kaip minėta pirmiau, ginčo nagrinėjimo metu nustatytos „Smart-ID" Paskyros Nr. 2 sukūrimo aplinkybės leidžia teigti, kad pareiškėja nesilaikė saugaus naudojimosi elektroninėmis paslaugomis rekomendacijų – besąlygiškai pasitikėjo tiek atsiųstame SMS pranešime nurodyta informacija, tiek ir pagal nuorodą atsidariusio interneto puslapio autentiškumu, jame pateikdama savo personalizuotus saugos duomenis.

Sprendžiant dėl pareiškėjos neatsargumo laipsnio, teisiškai reikšminga ir jos elgesio vertinimą lemianti aplinkybė, kad, ginčo byloje esančiais duomenis[10], pareiškėja, prieš suvesdama Paskyros Nr. 1 PIN2 slaptažodį, ne tik gavo ir matė pranešimą, raginantį įsitikinti, kad atliekamos operacijos informacija yra teisinga, bet ir pranešimą, informuojantį, jog šia operacija yra siekiama sukurti naują „Smart-ID" paskyrą, ir šiuose jos telefone pasirodžiusiuose

[9] https://www.swedbank.lt/private/d2d/ebanking/secureBanking?language=LIT

[10] Bankas kartu su papildomais paaiškinimais pateikė vidinių sistemų duomenis, kokio turinio standartiniai pranešimai klientams, besinaudojantiems „Smart-ID", kaip tapatybės patvirtinimo priemone, buvo siunčiami tuo laikotarpiu, kai buvo įvykdytos Operacijos, bei įrodymus, kad, prieš pareiškėjai suvedant „Smart-ID" Paskyros Nr. 1 PIN2 kodą, jai buvo išsiųstas ir rodomas pranešimas, informuojantis, kad suvesdama šios paskyros PIN2 kodą, ji tvirtina naujos „Smart-ID" paskyros sukūrimą: „Applying for new Smart-ID account" (liet. „Kreipiamasi dėl naujos „Smart-ID" paskyros").

programėlės „Smart-ID" pranešimuose pareiškėja turėjo paspausti „Patvirtinti" ir tik tada suvesti prašomą Paskyros Nr. 1 PIN2 slaptažodį. Bankas, remdamasis jo teiginius pagrindžiančiais vidaus sistemos duomenimis, nurodo, kad prašant suvesti Paskyros Nr. 1 PIN1 kodą, pareiškėjai buvo rodomas toks tekstas: „Patikrinkite teisingą kodą. Norėdami tęsti, įsitikinkite, kad Jūsų operacijos informacija yra teisinga. Jūs jungiatės prie Swedbank programėlės." Atsidarius Paskyros Nr. 1 ekranui, pareiškėja 21:20:26 val. suvedė tik pareiškėjai vienai žinomą Paskyrai Nr. 1 taikomą PIN1 slaptažodį, o 21:20:44 val. – ir Paskyros Nr. 1 PIN2 slaptažodį. Be to, prieš suvedant Paskyros Nr. 1 PIN2 kodą, pareiškėjai atsidariusiame programėlės „Smart-ID" pranešime buvo rodomas tekstas: „Norėdami tęsti, įsitikinkite, kad jūsų operacijos informacija yra teisinga", o patvirtinus šį pranešimą, ir veiksmo, kuriam pareiškėja davė sutikimą, aprašymas: „Applying for new Smart-ID account" (liet. „Kreipiamasi dėl naujos „Smart-ID" paskyros"). Neužbaigus Paskyros Nr. 2 sukūrimo proceso, bankas automatiškai išsiuntė SMS pranešimą pareiškėjos bankui nurodytu telefono numeriu – (*duomenys neskelbtini*): „New Smart-ID account has been created. If it was not done by you - please call us immediately to 1884 or +370 5 268 4444!"[11] (liet. „Jūsų vardu sukurta nauja Smart-ID paskyra. Jei tai buvote ne Jūs, nedelsiant paskambinkite 1884 ar +370 5 268 4444!"). Taigi, ginčo byloje esančiais duomenimis, pareiškėja savo mobiliajame įrenginyje esančioje programėlėje „Smart-ID" suvesdama PIN2 kodą turėjo matyti, jog šiuo veiksmu tvirtina naujos „Smart-ID" paskyros sukūrimą, nes tokia informacija pagal banko pateiktus įrodymus buvo rodoma pareiškėjos naudojamame įrenginyje „Smart-ID" programėlėje pasirodžiusiuose pranešimuose. Pareiškėja neginčija, kad PIN2 slaptažodį suvedė. Aplinkybė, kad pareiškėja neužtikrino savo personalizuotų saugumo duomenų konfidencialumo ir suvedė „Smart-ID" paskyros PIN2 kodą, faktiškai (kaip patvirtina ginčo byloje esantys įrodymai) turėdama matyti, kokiam veiksmui ji išreiškia savo sutikimą, lėmė tai, kad pareiškėjos vardu buvo ne tik sukurta nauja tapatybės patvirtinimo priemonės „Smart-ID" paskyra trečiųjų asmenų kontroliuojamame mobiliajame įrenginyje, bet ir iš pareiškėjos banko Sąskaitos įvykdytos dvi pareiškėjos neautorizuotos mokėjimo operacijos, kurias atliekant faktiškai pati pareiškėja nedalyvavo, joms savo sutikimo nedavė ir net nežinojo apie inicijavimo ir patvirtinimo aplinkybę.

Taigi, ginčo nagrinėjimo metu nustatyta aplinkybė, kad pareiškėja ne tik neužtikrino turimų mokėjimo priemonių personalizuotų saugumo duomenų konfidencialumo, bet ir neperskaičiusi „Smart-ID" programėlėje atsiradusių pranešimų turinio (pranešimuose nurodyto teksto), suvedė šios tapatybės patvirtinimo priemonės PIN1 ir PIN2 kodus, tokiais veiksmais patvirtindama „Smart-ID" Paskyros Nr. 2 sukūrimą trečiųjų asmenų kontroliuojamame įrenginyje. Toks pareiškėjos elgesys lėmė tai, kad banko taikyta saugesnio autentiškumo patvirtinimo procedūra šiuo atveju nebuvo pakankama, kad apsaugotų pareiškėją nuo sukčiavimo atakos ir neautorizuotos Operacijos iš jos Sąskaitos nebūtų įvykdytos.

Ginčo byloje esantys įrodymai ir pirmiau analizuotos ginčo nagrinėjimo metu nustatytos aplinkybės, susijusios tiek su pačios sukčiavimo atakos pobūdžiu, tiek su banko veiksmais, o svarbiausia – susijusios su pačios pareiškėjos veiksmais, net įvertinus ir tai, kad nagrinėjamo ginčo kontekste aktuali sukčiavimo ataka buvo sofistikuota ir ją pastebėti buvo būtinas pareiškėjos atidumas ir rūpestingumas, esant įrodymų, kad pareiškėjai siųstuose pranešimuose, prašančiuose suvesti Paskyros Nr. 1 PIN2 kodą, buvo rodoma tiksli ir teisinga informacija, dėl kokio veiksmo pareiškėja išreiškia sutikimą suvesdama PIN2 kodą, vis dėlto nesudaro pagrindo vertinti pareiškėjos elgesio tik kaip neatsargaus. Vertinimą, kad pareiškėjos elgesys, sudarant sąlygas tretiesiems asmenims užvaldyti jos Sąskaitą, buvo labai neatsargus, sustiprina ir aplinkybė, kad pareiškėja nesudvejojo trečiųjų asmenų banko vardu atsiųstame SMS pranešime be lietuviškų rašmenų nurodytos informacijos patikimumu ir nekvestionuodama pagal pranešime paspaustą nuorodą atsidariusio interneto puslapio autentiškumo, suvedė jame savo naudotojo ID ir asmens kodą, taip tretiesiems asmenims atskleisdama savo personalizuotus saugumo duomenis, įgalinusius trečiuosius asmenis inicijuoti naujos „Smart-ID" paskyros sukūrimą. Lietuvos banko vertinimu, pirmiau aptartos aplinkybės leidžia teigti, kad pareiškėja, nesilaikydama jai, kaip mokėjimo paslaugų vartotojai, nustatytų pareigų, susijusių su mokėjimo priemonės naudojimu, nebuvo tiek atidi ir rūpestinga, kiek akivaizdžiai buvo būtina nurodytomis aplinkybėmis – taigi, jei pareiškėja būtų laikiusis bent minimalių atsargumo ir dėmesingumo reikalavimų, ji būtų perskaičiusi jos naudojamoje tapatybės patvirtinimo priemonėje „Smart-ID" gautuose pranešimuose nurodytą tekstą, kad įvertintų, dėl

[11] Bankas paaiškino, kad pranešimas buvo išsiųstas anglų kalba, nes tokią kalbą, kurdami Paskyrą Nr. 2 programėlėje, pasirinko tretieji asmenys.

kokio veiksmo ji duoda sutikimą suvesdama PIN2 kodą, kas sukėlė jai teisines pasekmes. Toks pareiškėjos elgesys lėmė tai, kad tretieji asmenys įgijo galimybę sukurti naują „Smart-ID" paskyrą pareiškėjos vardu trečiųjų asmenų kontroliuojamame mobiliajame įrenginyje ir iš ten patvirtinti jų inicijuotas Operacijas. Tai suponuoja išvadą, kad pareiškėjos elgesys – būtinų saugumo rekomendacijų ir jai, kaip mokėjimo paslaugų vartotojai, nustatytų pareigų, naudojantis paslaugomis elektroninėje erdvėje, nesilaikymas, galiausiai lėmęs ir Operacijų įvykdymą bei jų sumų nurašymą iš pareiškėjos Sąskaitos banke, gali būti vertinamas kaip didelis pareiškėjos neatsargumas (aplaidumas), todėl visi nuostoliai, susiję su šių Operacijos įvykdymu, turėtų tekti pareiškėjai.

Įvertinus pirmiau išdėstytą informaciją, konstatuotina, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, kurioje nustatyta, kad mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai, jeigu jis jų patyrė dėl didelio neatsargumo neįvykdęs vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų, todėl, Lietuvos banko vertinimu, bankas neturi pareigos pareiškėjai grąžinti neautorizuotų Operacijų lėšų.

Dėl mokėjimo nurodymo neatšaukiamumo

Papildomai pažymėtina, kad pareiškėja kreipimesi teigia, kad sužinojusi, jog jos vardu sukurta nauja „Smart-ID" paskyra, nors tokių veiksmų atlikti ji nesiekė, ji bandė susisiekti su banku, tačiau to padaryti jai iškart nepavyko, nes telefono linija buvo užimta, o jos vardu sukurta nauja „Smart-ID" paskyra (Paskyra Nr. 2) buvo blokuota tik po antrojo jos pokalbio su banko darbuotoju. Vertinant banko veiksmų ir (ar) galimo neveikimo ryšį su pareiškėjos nuostoliais, įvykdžius Operacijas, būtina atkreipti dėmesį, kad nauja „Smart-ID" paskyra (Paskyra Nr. 2) pareiškėjos vardu trečiųjų asmenų kontroliuojamame įrenginyje buvo sukurta 21:20:57 val. – t. y. būtent tuo laiku bankas gavo informaciją apie pareiškėjos sutikimą (Paskyros Nr. 1 PIN2 suvedimą) sukurti Paskyrą Nr. 2. Banko vidinių sistemų duomenimis, 21:20:58 val. bankas išsiuntė SMS pranešimą į pareiškėjos telefoną, informuojantį ją apie naujos „Smart-ID" paskyros sukūrimą pareiškėjos vardu. Bankas nurodo, kad Operacijų įvykdymo dieną bankas taikė „Smart-ID" paskyros per „banklink" sąsają sukūrimo laiko atidėjimą – iki 2 minučių. Tai reiškia, kad per šį laikotarpį negavus prieštaravimo ir nesutikimo dėl naujos paskyros sukūrimo, nauja „Smart-ID" paskyra po nurodyto laikotarpio pradeda veikti ir ja galima naudotis, siekiant, be kita ko, ir inicijuoti bei patvirtinti mokėjimo operacijas. Pagal banko pateiktus duomenis, nagrinėjamu atveju bankas informaciją apie pareiškėjos vardu sukurtą Paskyrą Nr. 2 iš „SK ID Solution AS" gavo 21:23:57 val. – būtent nuo šio momento tretieji asmenys įgijo galimybę naudotis pareiškėjos vardu sukurta Paskyra Nr. 2, taip pat ir inicijuoti bei patvirtinti mokėjimo operacijas pareiškėjos vardu. Būtina pažymėti, kad pareiškėjos ginčijamos Operacijos buvo įvykdytos 21:27:30 val. ir atitinkamai 21:28:59 val., – taigi, dar iki pareiškėjos pirmo bandymo paskambinti į banką – 21:29 val.[12] Be to, priešingai, nei teigia pareiškėja kreipimesi į Lietuvos banką, remiantis ginčo byloje esančiais duomenimis, pareiškėjos naudojama tapatybės patvirtinimo priemonė – „Smart-ID" paskyra – buvo blokuota dar primojo pokalbio telefonu metu, t. y. su pareiškėja bendravęs darbuotojas 2021 m. rugsėjo 8 d. 21:37:11 val. užblokavo pareiškėjos vardu išduotas mokėjimo priemones (Paskyra Nr. 2 blokuota tą pačią dieną 21:43:56 val.). Vėliau (t. y. 21:38 val.) pareiškėja buvo sujungta su kitu banko darbuotoju, kuris paprašė patikslinti Operacijų įvykdymo aplinkybes. Atsižvelgiant į tai, kas nurodyta pirmiau, net ir tuo atveju, jei pareiškėja būtų buvusi iškart sujungta su banko darbuotoju jau pirmojo skambučio į banką metu, jos nedelsiant atliktas mokėjimo priemonių blokavimas šiuo atveju nebūtų padėjęs išvengti nuostolių pareiškėjai, nes, kaip minėta, sutikimas Operacijoms buvo duotas ir lėšos iš pareiškėjos Sąskaitos buvo nurašytos dar iki pirmojo pareiškėjos skambučio į banką.

Vertinant pareiškėjos, kaip mokėtojo, galimybę atšaukti mokėjimo nurodymą, 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

[12] Pirmo bandymo prisiskambinti į banką laikas nustatytas iš pareiškėjos kartu su papildomais paaiškinimais pateiktų jos mobiliojo telefono ekrano vaizdų – 2021 m. rugsėjo 8 d. skambučių išklotinės.

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 3.3.5 papunktyje nustatyta, kad mokėjimo nurodymas negali būti atšauktas po to, kai jį gauna bankas, išskyrus šiose sąlygose numatytus atvejus (3.3.5.1 papunktis); kai mokėjimo operacija inicijuojama gavėjo ar per gavėją (pvz., atsiskaitymas mokėjimo kortele), ar inicijuojama mokėjimo inicijavimo paslaugos teikėjo, mokėtojas negali atšaukti mokėjimo nurodymo po to, kai mokėjimo inicijavimo paslaugos teikėjui pateikė sutikimą inicijuoti mokėjimo operaciją arba mokėtojas gavėjui davė sutikimą atlikti mokėjimo operaciją. Tačiau jei atliekamas tiesioginis debetas, mokėtojas gali atšaukti tiesioginio debeto operacijos mokėjimo nurodymą vėliausiai iki dienos, einančios prieš dieną, kurią mokėtojas ir gavėjas susitarė nurašyti lėšas iš mokėtojo mokėjimo sąskaitos, pabaigos (3.3.5.2 papunktis); mokėjimo nurodymai, numatyti sąlygų 3.4.1.2 papunktyje (t. y. kai bankas ir mokėtojas susitaria dėl mokėjimo nurodymo įvykdymo konkrečią dieną ar konkrečiu momentu), gali būti atšaukti ne vėliau kaip iki banko darbo dienos, einančios prieš sutartą dieną, pabaigos (3.3.5.3 papunktis); pasibaigus banko mokėjimo paslaugų teikimo sąlygų 3.3.5.1–3.3.5.3 papunkčiuose nustatytiems terminams mokėjimo nurodymas gali būti atšauktas tik tuo atveju, kai dėl to susitaria klientas (mokėtojas) ir bankas, o sąlygų 3.3.5.2 papunktyje numatytais atvejais taip pat būtinas ir gavėjo sutikimas (3.3.5.4 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. Tai reiškia, kad bankas neturėjo pareigos, o šiuo atveju ir galimybės (atsižvelgiant į tai, kad Operacijos buvo įvykdytos kaip momentiniai kredito pervedimai) atšaukti pareiškėjos vardu pateiktų mokėjimo nurodymų įvykdyti Operacijas.

Todėl, įvertinus visa tai, kas išdėstyta pirmiau, ir ypač atsižvelgiant į tai, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, darytina išvada, kad pareiškėjos banko atžvilgiu keliamas reikalavimas grąžinti pareiškėjai dėl įvykdytų Operacijų iš jos Sąskaitos nurašytą 7 700 Eur sumą 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 pareiškėjos 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 arba kitą ginčų nagrinėjimo instituciją įstatymų nustatyta tvarka. Kreipimasis į teismą po Lietuvos banko sprendimo dėl ginčo esmės priėmimo nelaikomas šio sprendimo apskundimu.

Direktorius Arūnas Raišutis