LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

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

2022-04-28 Nr. 429-147
Vilnius

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

N u s t a t y t a:

2022 m. sausio 9 d. nuo 12 val. 28 min. iki 12 val. 33 min., panaudojant pareiškėjos vardu banko išduotos mokėjimo kortelės (toliau – Kortelė) duomenis, buvo inicijuotos 4 mokėjimo operacijos, kurių bendra suma – 1 533 Eur (toliau – mokėjimo operacijos), lėšas pervedant lėšų gavėjui *Binance* (toliau – gavėjas).

Pastebėjęs pareiškėjai nebūdingas mokėjimo operacijas ir siekdamas įsitikinti, kad mokėjimo operacijas inicijavo pati pareiškėja, bankas 2022 m. sausio 9 d. 14:37 val. susisiekė su pareiškėja telefonu ir pasiteiravo, ar pati pareiškėja inicijavo mokėjimo operacijas. Pareiškėja paaiškino, kad ji mokėjimo operacijų neinicijavo ir nedavė sutikimo jų įvykdyti. Tačiau pareiškėja teigė, kad į savo telefono numerį gavo SMS žinutę, kurioje pareiškėjai buvo pranešta, kad jos paskyra yra užblokuota ir kad norėdama ją atblokuoti pareiškėja turi spausti SMS žinutėje pateiktą aktyvią nuorodą. Paspaudusi šią nuorodą, pareiškėja pateko į interneto puslapį, vizualiai panašų į banko interneto puslapį, ir jame suvedė savo personalizuotus saugos duomenis (asmens kodą, banko atpažinimo kodą), kad prisijungtų prie savo su Kortele susietos sąskaitos, ir savo mobiliajame įrenginyje suvedė „Smart-ID" PIN1 kodą, kuriuo buvo patvirtintas prisijungimas prie banko mobiliosios programėlės iš kito įrenginio. Pareiškėja taip pat teigė, kad SMS žinutė buvo įsiterpusi į tikrų banko žinučių srautą, todėl ji manė, kad vykdo banko jai pateiktus nurodymus.

2022 m. sausio 10 d. gavusi banko sprendimą, kuriuo buvo informuota, kad bankas jai negrąžins mokėjimo operacijų lėšų, pareiškėja kreipėsi į Lietuvos banką dėl vartojimo ginčo nagrinėjimo. Kreipimesi pareiškėja paaiškino, kad 2022 m. sausio 9 d. į savo telefono numerį gavo SMS žinutę, kuri buvo įterpta į ankstesnių banko žinučių srautą. Minėtoje SMS žinutėje buvo pateikiama tokia informacija: „Jusu paskyra užblokuota. Noredami atblokuoti spauskite cia https://e-seb-prisijungti.com. Kitaip jusu saskaita bus uzdaryta." Kadangi SMS žinutė buvo įterpta į tikrų banko žinučių srautą, pareiškėja neturėjo pagrindo galvoti, kad SMS žinutę siuntė ne bankas, todėl paspaudė SMS žinutėje pateiktą aktyvią nuorodą ir buvo nukreipta į netikrą banko puslapį. „Suvedus atpažinimo bei asmens kodą išmetė klausimą dėl įtartinos operacijos ir paprašė patvirtinti su „Smart-ID", jeigu nepageidauju pervesti nurodytos sumos 1 000 Eur asmeniui X.X.. Operacijos atšaukimo patvirtinimui paprašė suvesti aštuonženklį „Smart-ID" kodą. Ekrane matėsi SEB banko puslapio langas kaip jungiantis įprastai. Suvedus „Smart-ID" kodą ilgai krovėsi, paskui atrodo, kad pasirodė žinutė, kad grąžins į pagrindinį puslapį." Pareiškėja teigia, kad į banko sistemas buvo įsilaužta, todėl be jos žinios ir sutikimo tretieji asmenys iš jos sąskaitos inicijavo mokėjimo operacijas.

Pareiškėja teigia, kad bankas, dar 2022 m. sausio 9 d. turėdamas informaciją, kad pareiškėja pati neinicijavo mokėjimo operacijų, 2022 m. sausio 10 d. jas įvykdė. Pareiškėja taip pat pažymėjo, kad „Smart-ID" PIN kodą suvedė tik vieną kartą, kad nebūtų įvykdyta 1 000 Eur mokėjimo operacija, tačiau iš jos sąskaitos buvo įvykdytos 4 mokėjimo operacijos.

Pareiškėja paaiškino, kad bankas jai pateikė atsakymą, kad negali grąžinti mokėjimo operacijų lėšų, net netyręs aplinkybių, ar nebuvo įsilaužta į banko vidines sistemas. Bankas, pareiškėjos nuomone, net nesiaiškino, kaip sukčių SMS žinutė pateko į tikrų banko žinučių srautą.

Pareiškėja teigė, kad mokėjimo operacijų lėšų gavėjas yra viena didžiausių kriptovaliutų keityklų Lietuvoje, be to, pats Lietuvos bankas yra pabrėžęs, kad sandoriai dėl kriptovaliutų pirkimo ir pardavimo yra vieni rizikingiausių. Pareiškėjos nuomone, bankas neturi įdiegęs pakankamų vidaus kontrolės procedūrų, nes prieš įvykdydamas mokėjimo operacijas lėšų gavėjui, užsiimančiam kriptovaliutų veikla, papildomai su pareiškėja nesusiekė telefonu ar interneto banku ir nepaklausė, ar pareiškėja norinti mokėjimo operacijų lėšas pervesti šiam gavėjui. Pareiškėjos nuomone, bankas neužtikrino savo atsiskaitymų sistemų saugumo ir neturi tinkamų vidaus kontrolės procedūrų, todėl turi prisiimti bent dalį pareiškėjos patirtų nuostolių. Pareiškėja prašė rekomenduoti bankui jai grąžinti dalį mokėjimo operacijų lėšų arba jas visas. Taip pat pareiškėja prašė ištirti, ar bankas turi įdiegęs pakankamas vidaus kontrolės procedūras, padedančias užtikrinti saugumą naudojantis banko teikiamomis mokėjimo paslaugomis.

Bankas nesutinka tenkinti pareiškėjos reikalavimo. Atsiliepime bankas nurodė atliekant tyrimą nustatytas mokėjimo operacijų inicijavimo ir įvykdymo aplinkybes. Bankas paaiškino, kad, kaip ir nurodė pati pareiškėja, ji 2022 m. sausio 9 d. į savo mobiliojo telefono numerį iš trečiųjų asmenų gavo SMS žinutę, kuria buvo informuota, kad jos interneto banko paskyra užblokuota. Pareiškėjos buvo prašoma paspausti SMS žinutėje pateiktą aktyvią nuorodą, kad paskyra būtų atblokuota. Kai paspaudė aktyvią nuorodą, pareiškėja buvo nukreipta į trečiųjų asmenų suklastotą banko interneto puslapį. Šiame puslapyje pareiškėja suvedė savo interneto banko atpažinimo kodą, asmens kodą ir savo mobiliajame įrenginyje, į savo „Smart-ID" paskyrą gavusi patvirtinimo užklausą, suvedė savo „Smart-ID" PIN1 kodą. Tokiais savo veiksmais pareiškėja suteikė tretiesiems asmenims galimybę sužinoti jos interneto banko atpažinimo kodą, asmens kodą ir „Smart-ID" PIN1 ir juos panaudojant (suvedant į banko programėlę, įdiegtą trečiųjų asmenų įrenginyje) pareiškėjos vardu prisijungti prie banko programėlės, įdiegtos trečiųjų asmenų naudojamame mobiliajame įrenginyje, inicijuoti ir tvirtinti veiksmus bei mokėjimo operacijas (tvirtinti mokėjimus, keisti operacijų limitus, peržiūrėti likučius, sudaryti sutartis, teikti prašymus ir pan.).

Banko teigimu, vėliau pareiškėja trečiųjų asmenų buvo nukreipta į kitą langą, kuriame, nepaisydama to, kad tuo momentu neinicijavo ir neketino atlikti jokios mokėjimo operacijos, suvedė savo Kortelės duomenis (Kortelės numerį, galiojimo datą ir CVV kodą). Pareiškėja šiais savo veiksmais (suvedusi savo interneto banko atpažinimo kodą, asmens kodą, savo mobiliajame įrenginyje į savo „Smart-ID" paskyrą gavusi patvirtinimo užklausą ir suvedusi savo „Smart-ID" PIN1 kodą bei suvedusi Kortelės duomenis (Kortelės numerį, galiojimo datą ir CVV kodą) suteikė tretiesiems asmenims galimybę pareiškėjos vardu atlikti mokėjimo operacijas.

Pastebėjęs pareiškėjai nebūdingas mokėjimo operacijas ir siekdamas įsitikinti, ar mokėjimo operacijas inicijavo pati pareiškėja, bankas susisiekė su pareiškėja telefonu ir informavo, kad banko vidaus sistemose buvo užfiksuoti bandymai atsiskaityti pareiškėjos Kortele. Paaiškėjus, kad pareiškėja mokėjimo operacijų neinicijavo, bankas užblokavo galimybę naudotis pareiškėjos Kortele ir pareiškėjos interneto banko paskyrą.

Atsiliepime bankas teigė, kad pareiškėja ir bankas, sudarydami Interneto banko ir Kortelės sutartis, susitarė dėl sutikimo įvykdyti mokėjimo operacijas, panaudojant Kortelę, davimo formos ir tvarkos. Atsiliepime nurodoma, kad banko vidaus sistemose buvo užfiksuoti duomenys, liudijantys, kad pareiškėjos mokėjimo operacijos buvo inicijuotos, suvedant Kortelės duomenis ir tik pareiškėjai žinomus prisijungimo prie interneto banko duomenis. Banko nuomone, pareiškėjos mokėjimo operacijos turi būti laikomos jos autorizuotomis, nes buvo duotas sutikimas jas atlikti banko ir pareiškėjos sutarta forma ir tvarka. Be to, pareiškėjos mokėjimo operacijos buvo atliktos ir patvirtintos, taikant saugesnę autentiškumo nustatymo procedūrą. Banko nuomone, nors Lietuvos Respublikos mokėjimų įstatyme reikalaujama mokėtojo sutikimo, kad mokėjimo operacija būtų laikoma autorizuota, tačiau toks sutikimas negali būti traktuojamas per plačiai, nes pats Mokėjimų įstatymas leidžia su mokėtoju susitarti dėl sutikimo įvykdyti mokėjimo operaciją formos. Mokėjimo operacijos įvykdymo sutikimo forma ir tvarka yra aiškiai nustatytos Banko mokėjimo paslaugų teikimo taisyklėse (toliau – Taisyklės). Banko nuomone „sutikimo faktui konstatuoti neturi būti remiamasi vien tik Klientės subjektyviąja puse, tačiau visų pirma, vertinami konkretūs Klientės atlikti veiksmai bei kaip jie atitinka „formos" kriterijų. Šio ginčo atveju, nėra jokių abejonių dėl formos bei dėl to, kad visus veiksmus – mokėjimo nurodymo suformavimui ir vykdymui būtinos informacijos pateikimą bei papildomo saugos sumetimais prašomo kodo atskleidimo veiksmus atliko pati Klientė."

Papildomai bankas atkreipė dėmesį, kad nustatytos aplinkybės leidžia vertinti pareiškėjos elgesį kaip itin neatsargų: pareiškėja paspaudė neaiškią nuorodą, suvedė savo interneto banko

atpažinimo kodą, asmens kodą, Kortelės duomenis ir savo mobiliajame įrenginyje savo atliekamus veiksmus patvirtino suvesdama tik jai žinomą „Smart-ID" PIN1 kodą. Banko teigimu, pareiškėja šiais veiksmais nesilaikė Mokėjimų įstatymo 34 straipsnyje aptartų mokėjimo paslaugų vartotojo pareigų, nes naudojosi mokėjimo priemone (interneto banku ir Kortele) ne pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, t. y. atskleidė Kortelės duomenis, suvedė prisijungimo duomenis (asmens kodą ir interneto banko atpažinimo kodą) ir savo mobiliajame įrenginyje savo veiksmus patvirtino suvesdama „Smart-ID" PIN1 kodą, todėl tretieji asmenys pareiškėjos vardu aktyvavo banko mobiliąją programėlę savo mobiliajame įrenginyje ir, turėdami Kortelės duomenis, pareiškėjos vardu patvirtino mokėjimo operacijas.

Banko teigimu, pareiškėja galėjo lengvai suprasti savo atliekamų veiksmų reikšmę ir pasekmes, nes tokius veiksmus atliko ne pirmą kartą – „Smart-ID" programėle naudojasi nuo 2019 metų, taip pat ne kartą yra atlikusi operacijas, kurioms inicijuoti yra naudojami Kortelės duomenys, o mokėjimo operacija patvirtinama 3D būdu. Todėl pareiškėjai turėjo būti žinoma tai, kad suvedus Kortelės duomenis iš su Kortele susietos mokėjimo sąskaitos bus nurašytos lėšos.

Bankas taip pat teigė, kad banko informacinėse sistemose yra užfiksuota, kad pareiškėja iš banko anksčiau buvo gavusi įspėjimą dėl sukčių siunčiamų pranešimų, tačiau jo nepaisė ir paspaudė sukčių atsiųstą nuorodą, neįsitikinusi, ar ji atitinka banko interneto banko svetainės adresą, kuriuo įprastai prisijungdavo ir inicijuodavo mokėjimo operacijas interneto banke. Bankas atkreipė dėmesį, kad, gavusi SMS pranešimą, kad jos interneto banko paskyra užblokuota, pareiškėja nesikreipė į banką, kad patikrintų SMS pranešime pateiktą informaciją, nors SMS žinutėje pateikta informacija apie užblokuotą paskyrą turėjo sukelti pagrįstų įtarimų. Banko teigimu, pareiškėjai nesukėlė įtarimų ir faktas, kad jos buvo prašoma suvesti „Smart-ID" PIN1 kodą norint atšaukti 1 000 eurų mokėjimo operaciją, kurios pareiškėja neinicijavo. Taip pat pareiškėja neįsitikino, ar interneto banko atpažinimo kodą, asmens kodą, Kortelės duomenis ir „Smart-ID" PIN1 kodą veda tikroje banko interneto svetainėje, o ne sukčių sukurtoje interneto svetainėje, kuri neatitiko banko interneto svetainės adreso. Banko nuomone, atsižvelgiant į tai, kad pareiškėja nesiekė nei gauti lėšų, nei įvykdyti mokėjimo operacijų, prašymas suvesti prisijungimo prie interneto banko duomenis, Kortelės duomenis ir „Smart-ID" PIN1 kodą pareiškėjai turėjo sukelti pagrįstų įtarimų, taigi, nepastebėti, kad suveda savo prisijungimo prie paskyros duomenis, pareiškėja galėjo tik dėl didelio savo aplaidumo (nerūpestingumo).

Bankas informavo, kad, pagal „MasterCard" organizacijos taisykles, mokėjimo operacijas galima ginčyti kaip atliktas neteisėtai, t. y. be mokėtojo žinios (angl. *fraud*), jeigu mokėjimo operacijos nėra autorizuotos (patvirtintos) „3D secure" kodu. Bankas nurodė, kad nagrinėjamu atveju, atsižvelgiant į tai, kad mokėjimo operacijos buvo patvirtintos „3D Secure" kodu, vadovaujantis „MasterCard" organizacijos taisyklėmis, ginčyti šių operacijų kaip neteisėtų, t. y. atliktų be pareiškėjos žinios, bankas neturi galimybės, nes neturi ginčo teisės.

Atsiliepime bankas prašo atmesti pareiškėjos 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.

Pareiškėjos ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjai pareiškėjos vardu banke atidarytoje sąskaitoje panaudojus Kortelės duomenis atliktų mokėjimo operacijų lėšų, iš viso – 1 533 Eur, sumą. Pareiškėja teigia neautorizavusi mokėjimo operacijų, tačiau ir neneigia trečiųjų asmenų suklastotame banko interneto puslapyje pati suvedusi savo prisijungimo prie paskyros duomenis. Pareiškėjos teigimu, tretieji asmenys be jos žinios ir sutikimo įgijo galimybę iš jos sąskaitos pasinaudojant Kortele įvykdyti mokėjimo operacijas,

nes bankas neužtikrino mokėjimo sistemų saugumo, neįvertino lėšų gavėjo rizikos lygio ir nesiėmė veiksmų, prieš įvykdant mokėjimo operacijas, įspėti pareiškėją, kad iš jos sąskaitos yra inicijuotos mokėjimo operacijos rizikinga kriptovaliutų veikla užsiimančiam lėšų gavėjui. Bankas teigia, kad pareiškėjos mokėjimo operacijos buvo tinkamai, t. y. šalių sutarta forma ir tvarka, autorizuotos, dėl to bankas jas pagrįstai įvykdė. Taip pat bankas teigia, kad yra sąlygos pareiškėjos elgesį, prarandant savo mokėjimo priemonę, vertinti kaip labai neatsargų, todėl bankas mano neturintis pareigos kompensuoti pareiškėjai jos patirtų nuostolių dėl mokėjimo operacijų. Dėl šių priežasčių, banko nuomone, visi mokėjimo operacijų nuostoliai turėtų tekti pareiškėjai.

Siekiant išspręsti tarp pareiškėjos ir banko kilusį ginčą, Lietuvos banko vertinimu, būtina nustatyti šias pagrindines aplinkybes: 1) ar mokėjimo operacijos laikytinos autorizuotomis, t. y. ar šioms operacijoms atlikti buvo gautas pareiškėjos sutikimas; 2) ar bankas turėjo (turi) pareigą grąžinti pareiškėjai mokėjimo operacijų sumas; 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 mokėjimo operacijų autorizavimo ir įvykdymo pagrįstumo

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 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) detalios tokio sutikimo davimo tvarkos. Vadovaujantis Mokėjimų įstatymo 13 straipsnio 3 dalies 3 punktu ir 29 straipsnio 1 punktu, mokėtojo sutikimo įvykdyti mokėjimo operaciją davimo sąlygos ir tvarka turi būti aptartos mokėtojo ir jo mokėjimo paslaugų teikėjo sudaromoje bendrojoje mokėjimo paslaugų teikimo sutartyje (toliau – bendroji sutartis).

Banko teigimu, pareiškėjos mokėjimo operacijos turi būti laikomos autorizuotomis, nes buvo atlikti veiksmai, reikalingi mokėjimo operacijoms Kortele inicijuoti, t. y. sutikimas suformuoti ir vykdyti mokėjimo operacijas buvo duotas vienu iš pareiškėjos ir banko sudarytoje bendrojoje sutartyje nurodytų būdų – panaudojant Kortelės duomenis (Kortelės numerį, galiojimo laiką, CVC kodą), suvedant interneto banko prisijungimo duomenis (interneto banko naudotojo atpažinimo kodą, asmens kodą) ir šiuos veiksmus patvirtinant suvedant atpažinimo priemonės „Smart-ID" PIN1 kodą). Atlikus minėtus veiksmus tretiesiems asmenims buvo suteikta galimybė pareiškėjos vardu prisijungti prie banko paskyros, kurią tretieji asmenys įdiegė savo mobiliajame įrenginyje, ir buvo suteikta galimybė inicijuoti ir tvirtinti veiksmus bei mokėjimo operacijas (tvirtinti mokėjimus, keisti operacijų limitus, peržiūrėti likučius, sudaryti sutartis, teikti prašymus ir pan.) iš pareiškėjos sąskaitos.

Kaip nurodo bankas atsiliepime, pareiškėja ir bankas, sudarydami Interneto banko sutartį bei Kortelės sutartį, susitarė dėl sutikimo įvykdyti mokėjimo operacijas, panaudojant Kortelę, davimo formos ir tvarkos. Mokėjimo operacijos patvirtinimo būdas, panaudojant Kortelę, aptartas banko Bendrųjų taisyklių (toliau – Taisyklės), kurios yra neatskiriama bet kurios banko ir jo kliento sudarytos sutarties dalis[1], 2 priede („Mokėjimo kortelių išdavimo ir

[1] Taisyklių 1 skyriaus nuostatos („Bendrosios taisyklės ir kainynas, kuriuos galite rasti tinklalapyje, taikomi teikiant visas mūsų paslaugas").

naudojimo taisyklės“), kurio 11 skyriuje nustatyta, kad mokėtojas duoda sutikimą mokėti mokėjimo kortele, jei: atsiskaito elektroninės prekybos ar paslaugų vietose ir įveda mokėjimo kortelės duomenis: mokėjimo kortelės numerį, galiojimo laiką, CVC kodą; pateikia mokėjimo kortelės ir (ar) savo duomenis prekybininkui ar paslaugos teikėjui ir patvirtina mokėjimo operaciją 3D būdu.

Atkreiptinas dėmesys į tai, kad Taisyklių 2 priedo 11 skyriuje kalbama apie atvejus, kai mokėtojas duoda savo sutikimą pervesti lėšas mokėjimo kortele prekybininkui arba paslaugų teikėjui, su kuriuo mokėtojas nori atsiskaityti, ir tuo tikslu perduoda mokėjimo kortelės ir kitus šioje Taisyklių nuostatoje nurodytus duomenis, nors nagrinėjamo ginčo atveju, priešingai, nei nurodyta minimoje Taisyklių nuostatoje, pareiškėja šiuos duomenis atskleidė ne dėl to, kad ketino Kortele pervesti lėšas gavėjui (atsiskaityti), o turėdama tikslą atblokuoti savo paskyrą, patikrinti įtartiną veiklą jos su Kortele susietoje sąskaitoje bei sustabdyti galimai neteisėtą bandymą nurašyti lėšas iš pareiškėjos banke atidarytos sąskaitos. Taigi, iš pareiškėjos pateiktų paaiškinimų ir iš ginčo byloje pateiktų duomenų, kurie pagrindžia pareiškėjos pateiktus paaiškinimus, galima teigti, kad savo valios inicijuoti ir įvykdyti mokėjimo operacijas pareiškėja neišreiškė ir nedavė tam savo sutikimo (neautorizavo mokėjimo operacijų) šalių sutarta forma ir tvarka.

Darydamas išvadą, kad mokėjimo operacijos buvo autorizuotos Taisyklėse nustatyta (šalių sutarta) tvarka, bankas iš esmės remiasi tik tuo faktu, kad mokėjimo operacijai įvykdyti buvo panaudoti Kortelės duomenys ir suvesti prisijungimo prie interneto banko prisijungimo duomenys, tačiau nevertina, kuriuo metu ir (arba) kas perdavė lėšų gavėjui ir (arba) jo mokėjimo paslaugų teikėjui duomenis, kurių pagrindu buvo inicijuotos mokėjimo operacijos, t. y. ar šiuos duomenis tiesiogiai pateikė pati pareiškėja, ar iš pareiškėjos šiuos duomenis neteisėtai išvilioję (mokėjimo priemonę neteisėtai pasisavinę) asmenys.

Iš ginčo byloje pateiktų ginčo šalių paaiškinimų ir banko vidaus sistemose užfiksuotų duomenų matyti, kad pareiškėja, trečiųjų asmenų suklastotame banko interneto puslapyje suvesdama savo prisijungimo duomenis (banko atpažinimo kodą ir asmens kodą) bei savo mobiliajame įrenginyje suvesdama „Smart-ID“ PIN1 kodą, suteikė tretiesiems asmenims galimybę pareiškėjos vardu prisijungti prie pareiškėjos banko paskyros, kurią tretieji asmenys, pasinaudodami iš pareiškėjos pasisavintais duomenimis, įdiegė kitame, ne pareiškėjai priklausančiame, mobiliajame įrenginyje, ir inicijuoti mokėjimo operacijas. Taip pat, banko Lietuvos bankui pateiktais sistemų duomenimis, mokėjimo operacijoms inicijuoti buvo panaudoti ir Kortelės duomenys (Kortelės numeris, galiojimo data ir CVV kodas) ir mokėjimo operacijos patvirtintos 3D būdu. Pareiškėja teigia Kortelės duomenų niekur nevedusi, Kortelė visą laiką buvusi jos žinioje. Taigi, banko pateikti duomenys patvirtina, kad mokėjimo operacijas inicijavo ne pati pareiškėja, o tretieji asmenys, neteisėtu būdu pasisavinę pareiškėjos prisijungimo prie paskyros bei Kortelės duomenis.

Nors bankas pateikė vidaus sistemose užfiksuotus duomenis, pagrindžiančius, kad mokėjimo operacijos buvo patvirtintos, taikant saugesnio autentiškumo patvirtinimo procedūrą, tačiau vien šie duomenys, Lietuvos banko vertinimu, neįrodo, kad mokėjimo operacijos buvo inicijuotos su pareiškėjos žinia ir sutikimu. Remiantis Mokėjimų įstatymo nuostatomis, tam, kad mokėjimo operacija būtų laikoma autorizuota, nepakanka vien to, kad mokėjimo operacija buvo patvirtinta šalių sutarta forma ir tvarka, svarbu nustatyti ir tai, ar atlikti konkrečią mokėjimo operaciją buvo duotas mokėtojo sutikimas, ypač atsižvelgiant į aplinkybę, kad mokėjimo operacija yra inicijuojama dėl trečiųjų asmenų neteisėtų veiksmų pasisavinus mokėtojo mokėjimo priemonę ir pasinaudojus šiais neteisėtu būdu įgytais duomenimis, inicijuojant mokėjimo operacijas be mokėtojo žinios ir sutikimo. Mokėjimų įstatymo 37 straipsnio 3 dalyje taip pat nustatyta, kad vien aplinkybė, jog mokėtojo mokėjimo paslaugų teikėjo vidaus sistemose užregistruotas mokėtojui išduotos mokėjimo priemonės, įskaitant jos personalizuotus saugumo duomenis, naudojimas, nebūtinai yra pakankamas įrodymas, kad mokėjimo priemone naudojosi ir (arba) mokėjimo operaciją autorizavo pats mokėtojas.

Siekdamas pagrįsti savo poziciją, t. y. kad mokėjimo operacijos buvo inicijuotos ir įvykdytos šalių sutarta forma ir tvarka, panaudojant tik pareiškėjai žinomus personalizuotus saugos duomenis, bankas pateikė savo vidaus sistemų išrašus, kurie patvirtina, kad siekiant prisijungti prie pareiškėjos paskyros buvo suvestas interneto banko naudotojo atpažinimo kodas, pareiškėjos asmens kodas, o pats prisijungimas prie pareiškėjos paskyros iš kito, ne pareiškėjai priklausančio, įrenginio buvo patvirtintas tik pareiškėjai žinomu atpažinimo priemonės „Smart-ID“ PIN1 kodu. Bankas taip pat pateikė duomenis, kad mokėjimo operacijos buvo inicijuotos suvedus Kortelės duomenis (Kortelės numerį, galiojimo laiką, CVC kodą). Be

to, iš ginčo byloje banko pateiktų duomenų matyti, kad mokėjimo operacijos buvo patvirtintos ne pareiškėjos turimame ir jos naudojamame (valdome) 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), o per trečiųjų asmenų valdomame mobiliajame įrenginyje pareiškėjos vardu suskurtą „Smart-ID" paskyrą.

Nors pareiškėja Lietuvos bankui teigė, kad, jos nuomone, buvo įsilaužta į banko sistemas ir todėl be pareiškėjos žinios ir sutikimo buvo įvykdytos mokėjimo operacijos, tačiau ginčo byloje nėra duomenų, kad mokėjimo operacijas būtų paveikę techniniai trikdžiai arba kiti banko teikiamos paslaugos trūkumai. Kaip ir minėta, banko pateikti duomenys įrodo, kad mokėjimo operacijų autentiškumas buvo patvirtintas, jos buvo tinkamai užregistruotos, įrašytos į sąskaitas, todėl nėra pagrindo teigti, kad bankas nepagrįstai įvykdė mokėjimo operacijas.

Įvertinus ginčo šalių pateiktus paaiškinimus bei remiantis ginčo byloje turimais įrodymais, kurie patvirtina, kad mokėjimo operacijų atlikimo dieną pareiškėjos vardu buvo sukurta „Smart-ID" paskyra kitame mobiliajame įrenginyje, kuris nepriklauso pareiškėjai ir nėra jos naudojamas, ir naudojantis šia paskyra buvo patvirtintos mokėjimo operacijos, galima daryti išvadą, kad mokėjimo operacijos buvo inicijuotos ir patvirtintos ne pačios pareiškėjos, o trečiųjų asmenų jiems neteisėtu būdu pasisavinus pareiškėjos mokėjimo priemonę, nors ir atitiko pareiškėjos ir banko sutartą sutikimo mokėjimo operacijoms Kortele davimo formą ir tvarką. Lietuvos banko vertinimu, vertinti pareiškėjos mokėjimo operacijų kaip autorizuotų – atliktų esant pačios pareiškėjos sutikimui (kaip tai suprantama Mokėjimų įstatymo 29 straipsnio 1 dalies kontekste), nėra pakankamo pagrindo, todėl Lietuvos bankas daro išvadą, kad pareiškėjos mokėjimo operacijos laikytinos neautorizuotomis.

Pareiškėja taip pat teigė, kad, jos nuomone, bankas turėjo įvertinti lėšų gavėjo riziką ir, prieš įvykdant mokėjimo operacijas, įspėti pareiškėją, kad iš jos sąskaitos yra inicijuotos mokėjimo operacijos rizikinga kriptovaliutų veikla užsiimančiam lėšų gavėjui. Mokėjimų įstatymo 43 straipsnio 3 dalyje nustatyta, kad kai įvykdytos visos mokėtojo ir mokėjimo paslaugų teikėjo bendrojoje sutartyje nustatytos sąlygos, mokėtojo sąskaitą tvarkantis mokėjimo paslaugų teikėjas negali atsisakyti įvykdyti mokėjimo nurodymo, nesvarbu, ar mokėjimo nurodymas inicijuotas mokėtojo, įskaitant inicijavimą per mokėjimo inicijavimo paslaugos teikėją, gavėjo ar per gavėją, išskyrus atvejus, kai tai draudžia kiti teisės aktai. Mokėjimų įstatymo 51 straipsnio 1 dalyje nustatyta, kad kai mokėjimo nurodymą tiesiogiai inicijuoja mokėtojas, jo mokėjimo paslaugų teikėjas atsako mokėtojui už tinkamą mokėjimo operacijos įvykdymą, nebent mokėtojo mokėjimo paslaugų teikėjas žino ir gali patvirtinti mokėtojui ir gavėjo mokėjimo paslaugų teikėjui, kad gavėjo mokėjimo paslaugų teikėjas gavo mokėjimo operacijos sumą, kaip nustatyta šio įstatymo 46 straipsnyje. Tokiu atveju gavėjo mokėjimo paslaugų teikėjas yra atsakingas gavėjui už tinkamą mokėjimo operacijos įvykdymą. Pagal Mokėjimų įstatymo 50 straipsnio 5 dalį, kai mokėtojas mokėjimo paslaugų teikėjui nurodo lėšų gavėjo mokėjimo paslaugų teikėjo sąskaitos numerį (unikalų identifikatorių), nesvarbu, kokius kitus lėšų gavėjų duomenis mokėtojas pateikė bankui (pvz., įmonės pavadinimas, adresas ar pan.), mokėjimo paslaugų teikėjai yra atsakingi mokėtojams už mokėjimo operacijų vykdymą pagal mokėtojų nurodytus lėšų gavėjų mokėjimo paslaugų teikėjų sąskaitos numerius. Finansinių paslaugų teikimą reglamentuojantys teisės aktai nenustato mokėjimo paslaugų teikėjams imperatyvios pareigos tikrinti mokėtojo pateiktų duomenų apie lėšų gavėją. Ginčo byloje turimais duomenimis, bankas mokėjimo operacijas įvykdė pagal jam mokėjimo nurodyme pateiktus lėšų gavėjo duomenis.

Įvertinus ginčo byloje turimus duomenis ir finansinių paslaugų teikimą reglamentuojančių teisės aktų nuostatas, nėra pagrindo teigti, kad bankas nepagrįstai įvykdė mokėjimo operacijas.

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

Vadovaujantis 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 pareiškėjos prisijungimo prie paskyros ir Kortelės duomenis tik todėl, kad pareiškėja dėl savo didelio neatsargumo neįvykdė Mokėjimų įstatymo 34 straipsnyje numatytų mokėtojo pareigų ir neužtikrino, kad be pareiškėjos, turinčios teisę naudotis mokėjimo priemone, personalizuotais saugumo duomenimis negalėtų pasinaudoti kiti asmenys.

Kad būtų galima įvertinti, ar pareiškėja iki mokėjimo operacijų įvykdymo galėjo pastebėti, kad mokėjimo priemonė buvo neteisėtai pasisavinta, svarbūs ne tik banko pateikti sistemų išrašų duomenys apie mokėjimo operacijų įvykdymą, bet ir ginčo šalių paaiškinimai apie mokėjimo priemonės praradimo ir mokėjimo operacijų įvykdymo aplinkybes. Vertinant ginčo šalių pateiktus paaiškinimus apie mokėjimo operacijų atlikimo aplinkybes, matyti, kad dalis ginčo šalių paaiškinimų apie aplinkybes, kuriomis tretieji asmenys neteisėtu būdu galėjo pasisavinti prisijungimo prie paskyros duomenis ir be pareiškėjos žinios ir sutikimo inicijuoti mokėjimo operacijas, sutampa. Tačiau nesutampa pareiškėjos ir banko pateikti paaiškinimai dėl Kortelės duomenų atskleidimo tretiesiems asmenims. Pareiškėja Lietuvos bankui telefonu teigė, kad savo Kortelės duomenų į trečiųjų asmenų suklastotą banko interneto puslapį nevedė, taip pat teigė, kad Kortelės duomenų nebuvo praradusi ir niekam jų nebuvo perdavusi. Tačiau banko pateikti sistemų išrašai patvirtina, kad visos mokėjimo operacijos buvo inicijuotos suvedus Kortelės duomenis ir jas papildomai patvirtinus 3D būdu.

Kaip minėta, ginčo byloje nustatyta, kad pareiškėja prarado savo prisijungimo prie paskyros personalizuotus saugos duomenis, kai prie paskyros jungėsi paspausdama SMS žinute į savo mobilųjį telefono numerį gautą aktyvią nuorodą ir taip pateko į netikrą banko interneto puslapį, kuriame suvedė savo banko atpažinimo kodą, asmens kodą ir patvirtino prisijungimą prie savo paskyros („Smart-ID" sukūrimą) iš kito, ne pareiškėjai priklausančio, įrenginio suvesdama „Smart-ID" PIN1 kodą. Šiuos duomenis nusavino tretieji asmenys ir savo mobiliojo telefono įrenginyje pareiškėjos vardu sukūrė naują paskyrą. Bankas teigia, kad, kai suvedė savo banko atpažinimo kodą, asmens kodą ir „Smart-ID" PIN1 kodą, pareiškėja trečiųjų asmenų buvo nukreipta į kitą interneto puslapį, kuriame suvedė savo Kortelės duomenis, o juos pasisavinę tretieji asmenys iš savo mobiliajame įrenginyje pareiškėjos vardu sukurtos paskyros inicijavo mokėjimo operacijas, kurios buvo patvirtintos 3D būdu. Kaip ir minėta, pareiškėja neigia vedusi Kortelės duomenis, tačiau banko sistemų išrašai šio pareiškėjos teiginio nepatvirtina, priešingai, įrodo, kad visos mokėjimo operacijos Kortele buvo inicijuotos panaudojus Kortelės duomenis. Taigi, ginčo byloje nesant pareiškėjos paaiškinimų apie jos atliktus veiksmus, dėl kurių ji prarado savo Kortelės duomenis, ir pareiškėjai teigiant, kad Kortelė visą laiką buvo jos žinioje, tačiau esant banko pateiktiems objektyviems duomenims – banko sistemų išrašams, kurie patvirtina, kad mokėjimo operacijos buvo inicijuotos panaudojus Kortelės duomenis ir jas patvirtinus 3D būdu, galima daryti išvadą, kad yra labiau tikėtina, kad pareiškėja tretiesiems asmenims atskleidė ne tik banko atpažinimo kodą, asmens kodą, „Smart-ID" PIN1 kodą, bet ir savo Kortelės duomenis (Kortelės numerį, galiojimo datą ir CVV kodą).

Iš pareiškėjos pateiktų paaiškinimų matyti, kad, vesdama savo banko atpažinimo kodą, asmens kodą ir „Smart-ID" PIN1 kodą, pareiškėja manė, kad tokiais savo veiksmais užkerta kelią iš jos sąskaitos įvykdyti jos neautorizuotą 1 000 Eur mokėjimo operaciją. Kaip ir minėta, pareiškėja, trečiųjų asmenų suklastome banko puslapyje suvedusi savo banko atpažinimo kodą ir savo asmens kodą, pamatė jai trečiųjų asmenų pateiktą žinutę, kurioje buvo nurodoma, kad jeigu pareiškėja nepageidauja pervesti nurodytos 1 000 Eur sumos asmeniui X.X., ji turi suvesti

savo „Smart-ID“ PIN1 kodą.

Teigdamas, kad pareiškėjos elgesys, dėl kurio ji prarado savo mokėjimo priemonę, turi didelio neatsargumo požymių, bankas remiasi tuo, kad pareiškėja nesilaikė mokėtojui nustatytos pareigos saugoti personalizuotus saugos duomenis ir niekam jų neatskleisti. Banko teigimu, pareiškėja paspaudė trečiųjų asmenų atsiųstą aktyvią nuorodą neįsitikinusi, ar ji atitinka banko interneto banko svetainės adresą, kuriuo ji įprastai prisijungdavo ir inicijuodavo mokėjimo operacijas interneto banke. Gavusi SMS žinutę, kad jos interneto banko paskyra yra užblokuota, pareiškėja nesikreipė į banką, kad patikrintų SMS žinutėje pateiktą informaciją, ir pasirinko spausti nežinomą aktyvią nuorodą. Pareiškėjai nesukėlė įtarimo ir faktas, kad jos buvo prašoma suvesti „Smart-ID“ PIN1 kodą, kad būtų atšaukta 1 000 Eur mokėjimo operacija, kurios ji pati neinicijavo, ir faktas, kad jos buvo prašoma suvesti Kortelės duomenis, nors pareiškėja jokios mokėjimo operacijos inicijuoti neketino. Banko teigimu, visi šie pareiškėjos veiksmai rodo didelį pareiškėjos neatsargumą, todėl ji neįvykdė Mokėjimų įstatymo 34 straipsnyje nustatytų mokėjimo paslaugų vartotojo pareigų, nes naudojosi mokėjimo priemone (interneto banku ir Kortele) ne pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, todėl tretieji asmenys pareiškėjos vardu aktyvavo banko mobiliąją programėlę savo mobiliajame įrenginyje ir, turėdami Kortelės duomenis, pareiškėjos vardu inicijavo ir patvirtino mokėjimo operacijas. Banko manymu, pareiškėja galėjo lengvai suprasti savo atliekamų veiksmų reikšmę ir pasekmes, nes tokius veiksmus atliko ne pirmą kartą. „Pareiškėja „Smart-ID“ programėle naudojasi nuo 2019 metų, taip pat ne kartą yra atlikusi operacijas, kurioms inicijuoti yra naudojami Kortelės duomenys, o patvirtinti – 3D būdas, todėl jai turėjo būti žinoma tai, kad suvedus Kortelės duomenis iš su Kortele susietos mokėjimo sąskaitos bus nurašytos lėšos.“

Lietuvos bankas atkreipia dėmesį, 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).

Ginčo byloje nustatytais duomenimis, tretieji asmenys neteisėtu būdu iš pareiškėjos pasisavino jos mokėjimo priemonę, pareiškėjai paspaudus SMS žinute į jos mobilųjį telefoną atsiųstą aktyvią nuorodą, įsiterpusią į tikrų banko žinučių srautą, ir patekus į trečiųjų asmenų suklastotą banko paskyrą, kurioje pareiškėja suvedė savo banko atpažinimo kodą, asmens kodą ir „Smart-ID“ PIN1 kodą. Kaip ir minėta, ginčo byloje nėra pareiškėjos paaiškinimų apie jos veiksmus, dėl kurių ji galėjo prarasti Kortelės duomenis. Tačiau banko pateikti sistemų išrašai neginčijamai patvirtina, kad mokėjimo operacijos buvo inicijuotos suvedus Kortelės duomenis ir jas patvirtinus 3D būdu, todėl yra labiau tikėtina, kad pareiškėja, kaip ir teigia bankas, Kortelės duomenis kartu su banko atpažinimo kodu, asmens kodu ir „Smart-ID“ PIN1 kodu suvedė patekusi į trečiųjų asmenų suklastotą banko paskyrą. Tretieji asmenys šiuos duomenis nusavino, kitame mobiliajame įrenginyje pareiškėjos vardu sukūrė naują paskyrą ir be pareiškėjos žinios ir sutikimo inicijavo mokėjimo operacijas.

Vertinant, ar pareiškėjos elgesys, kai ji paspaudė aktyvią nuorodą, atsiųstą SMS žinute

į jos mobilųjį telefoną, ir nepastebėjo, kad pateko į trečiųjų asmenų suklastotą banko paskyrą ir joje suvedė savo banko atpažinimo kodą, asmens kodą ir „Smart-ID" PIN1 kodą, gali būti vertinamas kaip labai neatsargus pareiškėjos elgesys, t. y. toks elgesys, dėl kurio mokėjimo priemonės turėtojo veiksmai iš esmės skiriasi nuo atsargaus elgesio reikalavimų, pažymėtina, kad vien tik faktas, kad pareiškėja paspaudė jai SMS žinute atsiųstą aktyvią nuorodą ir nepastebėjo, kad pateko ne į tikrą banko interneto puslapį, bet į trečiųjų asmenų suklastotą banko interneto puslapį, nereiškia pareiškėjos didelio neatsargumo. Nagrinėjamo ginčo atveju pareiškėją objektyviai galėjo suklaidinti ir kartu sumažinti jos budrumą tas faktas, kad pareiškėja SMS žinutę su aktyvia nuoroda gavo įterptą į kitų, tikrų, jai anksčiau banko siųstų žinučių srautą. Todėl normalu, kad pareiškėjai galėjo ir nebūti akivaizdu, kad SMS žinutę jai siuntė ne pats bankas, o tretieji asmenys.

Vis dėlto, vertinant tolimesnius pareiškėjos veiksmus, pareiškėjai paspaudus aktyvią nuorodą ir patekus į trečiųjų asmenų suklastotą banko puslapį, svarbu atkreipti dėmesį į tai, kad pareiškėjai pateikta pradinė informacija ir pradinis tikslas, dėl kurio pareiškėja spaudė aktyvią nuorodą, buvo paskyros atblokavimas. Būtent turėdama šį tikslą, pareiškėja suvedė savo banko atpažinimo kodą ir asmens kodą. Tačiau vėliau pareiškėjos buvo prašoma suvesti „Smart-ID" PIN1 kodą jau kitu tikslu – siekiant atšaukti 1 000 Eur mokėjimo pavedimą. Pareiškėjai faktas, kad iš pradžių jos buvo prašoma suvesti personalizuotus saugos duomenis, kad būtų atblokuota paskyra, o vėliau buvo prašoma suvesti „Smart-ID" PIN1 kodą, kad būtų atšaukta 1 000 Eur mokėjimo operacija, nesukėlė jokių įtarimų ir nepaskatino jos kreiptis į banką dėl informacijos patikslinimo.

Analizuojamų aplinkybių kontekste svarbu įvertinti ir tai, ar pareiškėja, suvesdama „Smart-ID" PIN1 kodą, galėjo suprasti, kad atlieka veiksmus, kurie gali lemti tam tikras teisines pasekmes, šiuo atveju – mokėjimo priemonės praradimą. Banko Taisyklių 2 priedo 11 punkte nėra įvardyta, kurio „Smart-ID" PIN kodo (PIN1 ar PIN2) suvedimas banko ir pareiškėjos santykiuose yra laikytinas sutikimo, kad iš pareiškėjos banko sąskaitos būtų atlikta mokėjimo operacija (mokėjimui mokėjimo kortele atlikti), 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." Vis dėlto nagrinėjamu atveju būtina įvertinti tai, kad pareiškėja, kaip ji pati teigia kreipimesi, savo prisijungimo prie interneto banko duomenis tretiesiems asmenims atskleidė ir savo „Smart-ID" paskyros PIN1 kodą trečiųjų asmenų paprašyta suvedė, tikėdama, kad tokiu veiksmu atšaukia galimai neteisėtą bandymą nurašyti lėšas iš pareiškėjos banko sąskaitos. Šiame kontekste svarbu tai, kad „Smart-ID" PIN kodas nėra naudojamas ir prašomas suvesti siekiant atšaukti mokėjimo operaciją, priešingai, „Smart – ID" PIN kodą prašoma suvesti siekiant patvirtinti mokėjimo operaciją. Pagal banko pateiktą informaciją, pareiškėja savo paskyra naudojosi aktyviai nuo 2019 m. ir turėjo patirties inicijuojant ir tvirtinant mokėjimo operacijas Kortele. Lietuvos banko nuomone, net jeigu pareiškėjai, paspaudus SMS žinute gautą aktyvią nuorodą ir suvedus savo banko atpažinimo kodą bei asmens kodą, nekilo įtarimų, kad tretieji asmenys tokiu būdu ketina pasisavinti jos mokėjimo priemonę, vis dėlto jai turėjo kilti pagrįstų įtarimų, kai jos buvo prašoma suvesti „SmartID" PIN 1 kodą siekiant atšaukti mokėjimo operaciją, nors pareiškėja, turėdama mokėjimo operacijų inicijavimo ir tvirtinimo „Smart-ID" kodu patirties, žinojo, kad „Smart-ID" PIN 1 kodu yra tvirtinamas mokėjimo operacijos vykdymas, o ne atšaukimas. Šiame kontekste, vertinant pareiškėjos elgesį, svarbi aplinkybė, kad, pareiškėjai suvedus Smart-ID" PIN 1 kodą, kad būtų atšaukta 1 000 Eur mokėjimo operacija, pareiškėjai atėjo banko žinutė, kad 1 000 Eur mokėjimo operacija buvo nesėkminga. Ginčo byloje pateiktais duomenimis, ši 1 000 Eur mokėjimo operacija buvo atmesta, nes pareiškėjos sąskaitoje nebuvo pakankamai lėšų. Taigi, suvedusi „Smart-ID" PIN 1 kodą, kad būtų atšaukta mokėjimo operacija, pareiškėja gavo žinutę, kad jos mokėjimo operacija nebuvo įvykdyta, tačiau į šią informaciją neatkreipė jokio dėmesio ir nemėgino kreiptis į banką, kad pasitikslintų informaciją. Ginčo byloje turimais duomenimis, būtent bankas pirmasis paskambino pareiškėjai ir pranešė, kad jos sąskaitoje yra vykdomos įtartinos mokėjimo operacijos, bet ne pati pareiškėja kreipėsi į banką.

Taigi, kaip matyti, pareiškėja, nei gavusi žinutę, kad jos paskyra yra užblokuota, nei

tada, kai sužinojo, kad 1 000 Eur mokėjimo operacija iš jos sąskaitos yra neįvykdyta, nesikreipė į banką, kad sužinotų, kodėl buvo užblokuota jos paskyra ir kodėl iš jos buvo vykdoma pareiškėjos neinicijuota 1 000 Eur mokėjimo operacija.

Lietuvos banko nuomone, jeigu pareiškėja būtų buvusi pakankamai atidi ir rūpestinga ir būtų atkreipusi dėmesį ne tik į tai, kad iš pradžių jos buvo prašoma suvesti personalizuotus saugos duomenis, kad paskyra būtų atblokuota, o vėliau buvo prašoma suvesti „Smart-ID" PIN 1 kodą jau kitu tikslu – kad mokėjimo operacija būtų atšaukta, nors pareiškėja turėjo nemažą naudojimosi „Smart-ID" patirtį, taigi, žinojo, kad „Smart-ID" PIN 1 kodas yra skirtas mokėjimo operacijoms tvirtinti, pareiškėja būtų pastebėjusi įtartinus veiksmus ir nuo jų susilaikiusi, tačiau ji elgėsi nerūpestingai ir toliau vykdė trečiųjų asmenų nurodymus, kurie objektyviai vertinant nebuvo logiški ir susiję. Pareiškėja netgi matydama trečiųjų asmenų jai pateiktą žinutę, kad iš jos sąskaitos ketinama įvykdyti 1 000 Eur mokėjimo operaciją, nemėgino susiekti su banku, kad pasitikslintų, kas ir kodėl iš jos sąskaitos inicijuoja mokėjimo operaciją, nors ji nedavė sutikimo jos atlikti.

Kaip ir minėta, banko pateikti sistemų išrašai patvirtina, kad visos mokėjimo operacijos buvo įvykdytos panaudojus pareiškėjos Kortelės duomenis ir patvirtintos 3D būdu. Kadangi pareiškėja Lietuvos bankui neteikė paaiškinimų, kaip tretieji asmenys galėjo pasisavinti jos Kortelės duomenis, todėl ginčo byloje nėra pareiškėjos paaiškinimų, iš kurių būtų galima vertinti jos aplaidumo, dėl kurio pareiškėja prarado savo mokėjimo priemonės – Kortelės duomenis, laipsnį. Vis dėlto turimi įrodymai patvirtina, kad Kortelės duomenys inicijuojant mokėjimo operacijas buvo panaudoti, mokėjimo operacijos buvo patvirtintos 3D būdu. Vadinasi, pareiškėja turėjo tretiesiems asmenims perduoti Kortelės duomenis. Bankas teigia, kad Kortelės duomenys buvo suvesti kartu su banko atpažinimo kodu, asmens kodu ir „Smart-ID" PIN1 kodu. Atsižvelgiant į tai, galima daryti išvadą, kad yra labiau tikėtina, kad pareiškėja Kortelės duomenis suvedė tame pačiame trečiųjų asmenų suklastotame banko puslapyje, kuriame, kaip pati pripažino, suvedė banko atpažinimo kodą, asmens kodą ir „Smart-ID" PIN1 kodą.

Taisyklių 2 priedo 11 skyriuje nustatyta, kad mokėtojas duoda sutikimą mokėti mokėjimo kortele, jei atsiskaito elektroninės prekybos ar paslaugų vietose ir įveda mokėjimo kortelės duomenis: mokėjimo kortelės numerį, galiojimo laiką, CVC kodą; pateikia mokėjimo kortelės ir (ar) savo duomenis prekybininkui ar paslaugos teikėjui ir patvirtina mokėjimo operaciją 3D būdu.

Pareiškėja turėjo ir galėjo suprasti, kad Kortelės duomenų suvedimas ir „Smart-ID" PIN1 kodo suvedimas yra skirti duoti sutikimą įvykdyti mokėjimo operaciją, bet ne ją atšaukti, kaip teigia maniusi pareiškėja. Lietuvos banko vertinimu, pareiškėja, jeigu tik būtų buvusi pakankamai atidi ir rūpestinga, galėjo pastebėti savo mokėjimo priemonės praradimą, nes jai akivaizdžiai turėjo sukelti įtarimų faktas, kad jos buvo prašoma suvesti personalizuotus saugos duomenis, reikalingus mokėjimo operacijai įvykdyti, o ne atšaukti. Tačiau pareiškėja elgėsi nerūpestingai ir, matydama trečiųjų asmenų jai pateiktą žinutę, kad iš jos sąskaitos yra mėginama atlikti jos neinicijuotą 1 000 Eur mokėjimo operaciją gavėjai X.X., nesikreipė į banką, kad pasiteirautų, kas ir kodėl be jos žinios ir sutikimo inicijuoja mokėjimo operaciją iš jos sąskaitos, o vietoje to suvedė visus jos trečiųjų asmenų prašomus suvesti duomenis, kuriuos tretieji asmenys neteisėtu būdu pasisavino ir be pareiškėjos žinios ir sutikimo inicijavo mokėjimo operacijas. Lietuvos banko vertinimu, toks pareiškėjos elgesys gali būti pripažintas kaip elgesys, iš esmės besiskiriantis nuo atsargaus elgesio reikalavimų, jis galiausiai ir lėmė tai, kad pareiškėja prarado savo mokėjimo priemonę.

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 pareiškėja mokėjimo priemone naudojosi nesilaikydama mokėjimo priemonės išdavimą ir naudojimą reglamentuojančių sąlygų, o sužinojusi apie neautorizuotą mokėjimo

priemonės naudojimą (1 000 Eur mokėjimo operaciją, kurią buvo prašoma atšaukti), nesikreipė į banką ir bankui nepranešė, kad kažkas iš jos sąskaitos ketina vykdyti 1 000 Eur mokėjimo operaciją, kurios ji pati neinicijavo, tačiau yra prašoma ją atšaukti, mokėjimo operacijos atšaukimui panaudojant personalizuotus saugos duomenis, kurie reikalingi mokėjimo operacijai inicijuoti. Galima teigti, kad pareiškėja 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 pareiškėjos veiksmai, dėl kurių ji prarado mokėjimo priemonę, pasireiškė dideliu neatsargumu, tai galiausiai ir lėmė, kad neautorizuotos mokėjimo operacijos buvo įvykdytos ir buvo patirti nuostoliai. Lietuvos banko nuomone, įvertinus pirmiau išdėstytas aplinkybes ir padarytas išvadas, galima teigti, kad pareiškėja iki mokėjimo operacijos įvykdymo galėjo pastebėti, kad jos 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 pareiškėjos sukčiavimas arba didelis neatsargumas. Kaip ir buvo minėta, Lietuvos banko nuomone, nagrinėjamo ginčo atveju pareiškėjos elgesys, dėl kurio ji prarado savo mokėjimo priemonę, gali būti laikomas labai neatsargiu, iš esmės ir nulėmusiu neautorizuotų mokėjimo operacijų iš pareiškėjos sąskaitos įvykdymą. Įvertinus pirmiau išdėstytą informaciją, konstatuotina, kad yra pagrindo pareiškėjai taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį. Lietuvos banko vertinimu, pareiškėjos reikalavimas bankui grąžinti neautorizuotų mokėjimo operacijų lėšų sumą yra nepagrįstas, todėl atmestinas.

Dėl mokėjimo nurodymų įvykdyti mokėjimo operacijas atšaukimo

Pareiškėja kreipimesi teigia, kad, bankui su ja susiekus ir informavus, kad iš jos sąskaitos yra inicijuotos mokėjimo operacijos, pareiškėja banko prašė jas atšaukti ir nepervesti mokėjimo operacijų lėšų gavėjui. Pareiškėja atkreipė dėmesį, kad pokalbio su banku metu lėšos su Kortele susietoje sąskaitoje dar buvo tik rezervuotos, tačiau nenurašytos, todėl bankas, pareiškėjos vertinimu, pareiškėjos vardu pateiktus mokėjimo nurodymus įvykdyti mokėjimo operacijas turėjo galimybę atšaukti ir lėšų į trečiųjų asmenų sąskaitą nepervesti, tačiau to nepadarė.

Atsižvelgiant į tai, papildomai 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, mokėjimo nurodymai įvykdyti mokėjimo operacijas buvo pateikti prieš bankui kreipiantis į pareiškėją su pranešimu apie įtartinas mokėjimo operacijas iš pareiškėjos sąskaitos, o pareiškėjos prašymas atšaukti mokėjimo operacijas bankui buvo pateiktas po to, kai mokėjimo nurodymus jau buvo gavęs bankas, todėl Mokėjimų įstatyme nustatymas mokėjimo nurodymo atšaukimo terminas jau buvo praėjęs, todėl bankas atšaukti pareiškėjos mokėjimo operacijų nebegalėjo.

Bankas taip pat paaiškino, kad, vadovaujantis mokėjimo kortelių organizacijos „MasterCard" taisyklėmis, inicijavus ir priėmus vykdyti mokėjimo operacijas, atliktas mokėjimo kortele, lėšos su kortele susietoje sąskaitoje, siekiant užtikrinti vėlesnį lėšų nurašymą, pirmiausiai yra rezervuojamos. Kai klientas suveda mokėjimo kortelės duomenis ir patvirtina mokėjimo operaciją prisijungimo priemone, mokėjimas jau būna įvykdytas ir lėšų rezervacijos

panaikinimas (t. y. pinigų pervedimas prekybininkui) negali būti atšauktas. Šią banko poziciją patvirtina ir banko Taisyklių 13 skyriaus nuostatos, pagal kurias, davus sutikimą mokėjimo operacijai banko išduota mokėjimo kortele, bankas lėšas pirmiausia rezervuoja su mokėjimo kortele susietoje sąskaitoje. Remiantis 13 skyriaus nuostatomis, bankas atšaukia lėšų rezervavimą su mokėjimo kortele susietoje sąskaitoje, jei per 15 kalendorinių dienų nuo lėšų rezervavimo datos iš lėšų gavėjo bankas negauna patvirtinimo apie atsiskaitymą mokėjimo kortele. Vadinasi, bankas gali panaikinti (ir panaikina) lėšų rezervaciją tik tuo atveju, jei gaunamas lėšų gavėjo sutikimas dėl mokėjimo nurodymo atšaukimo arba lėšų gavėjo bankas nustatytais terminais nepateikia patvirtinimo apie atsiskaitymą mokėjimo kortele. Atkreiptinas dėmesys, kad tokios aplinkybės nagrinėjamo ginčo atveju nebuvo nustatytos, taigi, nebuvo nustatytos ir sąlygos, kada pagal Taisyklių sąlygas mokėjimo operacijoms, patvirtintoms šalių sutartu būdu, įvykdyti pritaikytą lėšų rezervaciją bankas gali panaikinti.

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 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.

Direktorius Arūnas Raišutis