LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

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

2022-12-21 Nr. 429-653
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:

Pareiškėja 2022 m. birželio 18 d. 14 val. 36 min. telefonu gavo SMS pranešimą su nuoroda. Paspaudus trečiųjų asmenų atsiųstą nuorodą, atsidarė netikras banko interneto puslapis, imituojantis banko interneto banko puslapį, jame buvo prašoma įvesti pareiškėjai asmeniškai suteiktus unikalius duomenis – interneto banko atpažinimo kodą ir asmens kodą, būtinus prisijungti prie interneto banko, o vėliau suvesti ir pareiškėjos naudojamos atpažinties priemonės „Smart-ID" paskyros PIN1 kodą. Suvedus minėtus duomenis, tretieji asmenys prisijungė prie pareiškėjos interneto banko paskyros ir pareiškėjos vardu iš jos sąskaitos banke inicijavo 1 733 Eur vertės mokėjimą, kuris buvo patvirtintas suvedant pareiškėjos naudojamos atpažinties priemonės „Smart-ID" paskyros PIN2 kodą (toliau – Mokėjimas).

2022 m. birželio 18 d. 15:10 val. pareiškėja kreipėsi į banką telefonu, norėdama pranešti apie sukčiavimo atvejį. Telefoninio pokalbio metu banko darbuotoja užblokavo pareiškėjos interneto banko paskyrą.

2022 m. birželio 20 d. bankas kreipėsi į lėšų gavėjo mokėjimo paslaugų teikėją *Verse Payments Lithuania UAB* dėl Mokėjimo sumos grąžinimo, tačiau lėšų gavėjo mokėjimo paslaugų teikėjas bankui pateikė atsakymą, kad gavėjo sąskaitoje lėšų nebėra.

Pareiškėja, ginčydama banko sprendimą nekompensuoti jos nuostolių dėl įvykdyto Mokėjimo, kreipėsi į Lietuvos banką dėl ginčo nagrinėjimo.

Kreipimesi pareiškėja teigė, kad prie jos banko sąskaitos neteisėtai prisijungė tretieji asmenys ir jos vardu inicijavo 1 733 Eur Mokėjimą. Pareiškėja teigė, kad Mokėjimo pati neinicijavo, tačiau paspaudė jai SMS žinute sukčių atsiųstą nuorodą ir į sukčių suklastotą interneto banko puslapį suvedė savo interneto banko atpažinimo kodą ir asmens kodą. Pareiškėja teigė neatsimenanti, ar vedė „Smart-ID" PIN1 ir PIN2 kodus. Pareiškėjos teigimu, bankas nepagrįstai įvykdė Mokėjimą, nors jis pareiškėjos nebuvo autorizuotas. Kreipimesi pareiškėja prašo rekomenduoti bankui kompensuoti pareiškėjai jos ginčijamo Mokėjimo sumą.

Bankas nesutinka tenkinti pareiškėjos reikalavimo, nes ji elgėsi itin neapdairiai: paspaudė neaiškią nuorodą, suvedė savo interneto banko ID, asmens kodą ir savo mobiliajame įrenginyje savo atliekamus veiksmus patvirtino suvesdama tik jai žinomus „Smart-ID" paskyros PIN1 ir PIN2 kodus, dėl to tretieji asmenys galėjo ne tik pareiškėjos vardu inicijuoti Mokėjimą, bet ir ginčijamas Mokėjimas buvo tinkamai patvirtintas.

Atsiliepime pažymima, kad nors pareiškėja teigia neautorizavusi Mokėjimo, tačiau banko sistemų išrašai rodo, kad Mokėjimas buvo patvirtintas tik pareiškėjai žinomu „Smart-ID" PIN2 kodu, o prieš vedant PIN2 kodą pareiškėjai buvo rodoma ir Mokėjimo suma bei gavėjo duomenys. Banko nuomone, Mokėjimas turi būti laikomas pareiškėjos autorizuotu. Mokėjimo operacijoms tvirtinti bankas taiko papildomą kliento ir jo operacijų autentifikavimą, taip siekdamas suteikti galimybę klientui įsitikinti inicijuojamos operacijos teisėtumu. Klientams įvykdžius visas banko ir kliento sutartas sąlygas, kad kliento inicijuota operacija būtų tinkamai identifikuota, bankas įsipareigoja tokias operacijas įvykdyti. Bankas nurodo, kad vykdant Mokėjimą banko sistemos veikė saugiai, jokių sutrikimų užfiksuota nebuvo. Įvertinęs aplinkybių visumą ir teisinį reglamentavimą, bankas mano neturintis pareigos pareiškėjai kompensuoti

nuostolių, patirtų dėl įvykdyto Mokėjimo.

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. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Pareiškėjos ir banko ginčas kilo dėl banko atsisakymo grąžinti ir (ar) kompensuoti pareiškėjai jos ginčijamo Mokėjimo, įvykdyto dėl trečiųjų asmenų surengtos sukčiavimo atakos, sumą.

Pareiškėja teigia, kad bankas įvykdė neautorizuotą mokėjimo operaciją, nes pareiškėja pati jos neinicijavo ir nepatvirtino. Bankas teigia, kad tretieji asmenys įgijo sąlygas inicijuoti Mokėjimą tik dėl to, kad pareiškėja dėl didelio neatsargumo atskleidė savo mokėjimo priemonių personalizuotus saugumo duomenis tretiesiems asmenims ir Mokėjimą patvirtino suvesdama savo naudojamos „Smart-ID" paskyros PIN2 kodą, todėl Mokėjimo lėšų grąžinti ir (ar) kompensuoti pareiškėjai bankas neturi pareigos.

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.

Lietuvos banko vertinimu, siekiant išspręsti tarp pareiškėjos ir banko kilusį ginčą bei pasisakyti dėl pareiškėjos keliamo reikalavimo pagrįstumo, būtina nustatyti, ar: 1) Mokėjimas laikytinas autorizuotu; 2) bankas turėjo (turi) pareigą grąžinti (kompensuoti) pareiškėjai Mokėjimo sumą.

1. Dėl ginčijamo Mokėjimo 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).

Ginčo šalių sutartinių santykių neatskiriama dalimi esančių banko Bendrųjų taisyklių 1 priedo 3 skyriuje nustatyta, kad sutikimą atlikti mokėjimo operaciją mokėtojas gali duoti "<…> patvirtindamas elektroniniu parašu, naudodamas mūsų suteiktas atpažinimo priemones (slaptažodžius, kodus, kitus personalizuotus saugumo duomenis) interneto banke arba SEB mobiliojoje programėlėje, kitu su mumis sutartu ar banko nustatytu būdu."

Bankas, darydamas išvadą, kad Mokėjimui atlikti buvo tinkamai, taigi, šalių sutarta tvarka, išreikštas pareiškėjos sutikimas, remiasi banko vidinės sistemos duomenimis, kurie

patvirtina, kad Mokėjimui įvykdyti buvo panaudoti pareiškėjos interneto banko prisijungimo duomenys – interneto banko naudotojo ID kodas ir pareiškėjos vardu išduotos atpažinimo priemonės „Smart-ID" PIN1 (prisijungti prie interneto banko) ir PIN2 (patvirtinti Mokėjimą) kodai. Atsižvelgdamas į tai, kad Mokėjimas buvo patvirtintas šalių sutartu būdu, taikant griežtą kliento tapatybės nustatymo procesą, bankas mano, kad nėra pagrindo laikyti Mokėjimo neautorizuotu.

Darydamas išvadą, kad Mokėjimas buvo tinkamai pareiškėjos patvirtintas ir laikytinas autorizuotu, bankas papildomai nevertino Mokėjimo inicijavimo ir patvirtinimo aplinkybių: kas perdavė lėšų gavėjui ir (arba) jo mokėjimo paslaugų teikėjui duomenis, kurių pagrindu buvo inicijuotas Mokėjimas, t. y. ar šiuos duomenis tiesiogiai pateikė pati pareiškėja, ar iš pareiškėjos šiuos duomenis neteisėtai išvilioję tretieji asmenys. Lietuvos banko vertinimu vien faktas, kad Mokėjimas papildomai patvirtintas pagal griežtą tapatybės nustatymo procesą, t. y. papildomai suvedus tik pareiškėjai žinomą jos naudojamos tapatybės patvirtinimo priemonės „Smart-ID" paskyros PIN2 kodą, savaime dar nereiškia, kad Mokėjimas buvo atliktas su pareiškėjos sutikimu.

Siekdamas pagrįsti teiginį, kad Mokėjimams atlikti buvo tinkamai, t. y. šalių sutartu būdu, duotas pareiškėjos sutikimas, bankas remiasi pirmiau aptartomis banko Bendrųjų taisyklių nuostatomis. Vis dėlto minėtose banko Bendrųjų taisyklių nuostatose kalbama apie atvejus, kai *mokėtojas* duoda savo sutikimą pervesti lėšas ir tuo tikslu panaudoja jam išduotas mokėjimo ir tapatybės patvirtinimo priemones (jų duomenis). Tačiau nustatyta, kad pareiškėja, priešingai, nei nurodyta aptariamose nuostatose, savo prisijungimo prie interneto banko duomenis panaudojo fiktyvioje – į telefoną gautoje SMS žinutėje pateiktą nuorodą paspaudus atsiradusioje, interneto svetainėje ir suvedė juos ne dėl to, kad ketino pervesti lėšas, siekdama atsiskaityti už suteiktas paslaugas ar įsigytas prekes, o vykdydama gautoje žinutėje pateiktus nurodymus ir siekdama atlikti veiksmus, kad tariamai būtų atblokuota paskyra.

Lietuvos banko vertinimu, tais atvejais, kai nustatomi duomenys, kad mokėtojo (vartotojo) per neatsargumą atskleistais mokėjimo priemonių personalizuotais saugumo duomenimis neteisėtai pasinaudoja tretieji asmenys ir mokėtojo vardu juos pateikia tam, kad būtų inicijuotas mokėjimo nurodymas atlikti lėšų pervedimo operaciją, tokios mokėjimo operacijos negali būti laikomos operacijomis, kurioms įvykdyti buvo duotas mokėtojo sutikimas Mokėjimų įstatymo 29 straipsnio 1 dalies prasme. Trečiojo asmens veiksmai, kuriais pateikiamas mokėjimo nurodymas įvykdyti lėšų pervedimo operaciją mokėtojo vardu, nors formaliai ir atitinka mokėtojo ir mokėjimo paslaugų teikėjo sutartą sutikimo atlikti mokėjimo operaciją davimo formą, negali būti laikomi tinkamu mokėtojo sutikimu atlikti tokią mokėjimo operaciją, esant duomenims, kad jie neatitinka mokėtojo tikrosios valios.

Bankas atsiliepime taip pat teigia, kad sutikimo faktui konstatuoti neturi būti remiamasi vien tik pareiškėjos subjektyviu vertinimu dėl to, ar Mokėjimas laikytinas autorizuotu, tačiau turi būti vertinami konkretūs pareiškėjos atlikti veiksmai ir ar jie atitinka su banku sutartos sutikimo atlikti mokėjimo operaciją kriterijų.

Atsižvelgdamas į šiuos banko teiginius, Lietuvos bankas pažymi, kad, kaip buvo nurodyta pirmiau, vien tik aplinkybė, jog mokėtojo mokėjimo paslaugų teikėjo vidaus sistemose užregistruotas mokėtojui išduotos mokėjimo priemonės, įskaitant jos personalizuotus saugumo duomenis, naudojimas, nelaikytina pakankamu įrodymu, jog mokėjimo priemone tikrai naudojosi pats vartotojas ir (arba) kad tokia mokėjimo operacija laikytina tinkamai mokėtojo autorizuota. Nesant objektyvių įrodymų, kad, inicijuojant šalių sutartu būdu patvirtintą ir vartotojo ginčijamą mokėjimo operaciją, vartotojo mokėjimo priemone ir jos personalizuotais saugumo duomenimis be vartotojo žinios ir valios galėjo pasinaudoti tretieji asmenys, ir esant tik subjektyviems vartotojo paaiškinimams, įprastai tokia mokėjimo operacija laikytina autorizuota.

Lietuvos bankas pažymi, kad valia yra esminis kiekvienos sandorio, kaip teisinio veiksmo, kuriuo siekiama sukurti tam tikras teises ir pareigas, elementas[1]. Tai reiškia, kad, nesant mokėtojo valios inicijuoti lėšų pervedimo operacijos, toks mokėjimo nurodymas, nors formaliai ir patvirtintas šalių sutarta sutikimo atlikti mokėjimo operaciją davimo forma, negali būti laikomas tinkamai autorizuotu paties mokėtojo, turint duomenų, kad tokiam mokėjimo nurodymui pateikti pats mokėtojas savo valios neišreiškė, nesuprato, o tam tikrais atvejais ir

[1] „Apgaulės atveju sudarytas sandoris yra ne sandorio šalies laisvos valios išraiškos rezultatas, o kitos sandorio šalies ar trečiojo asmens nesąžiningų veiksmų rezultatas. Jeigu apgaulės nebūtų buvę, apgautoji sandorio šalis sandorio arba apskritai nebūtų sudariusi, arba būtų sudariusi jį visiškai kitokiomis sąlygomis." (Lietuvos Aukščiausiojo Teismo 2016 m. gegužės 12 d. nutartis civilinėje byloje Nr. 3K-3-268-421/2016).

negalėjo žinoti, kad jo vardu yra pateikiamas mokėjimo nurodymas pervesti lėšas.

Mokėtojo valia pateikti konkretų mokėjimo nurodymą mokėjimo paslaugų teikėjui yra esminė aplinkybė, vertinant, ar ginčijama mokėjimo operacija laikytina autorizuota, tačiau, kaip minėta pirmiau, tinkama mokėtojo valios išraiškos forma vertintina ne tik vertinant mokėtojo nuomonę, teiginius apie mokėjimo nurodymo pateikimo ir ginčijamos mokėjimo operacijos įvykdymo aplinkybes, tačiau analizuotinos ir mokėtojo valios išraišką atspindinčios ir pagrindžiančios mokėjimo nurodymo pateikimo ir ginčijamos mokėjimo operacijos įvykdymo aplinkybės. Tais atvejais, kai ginčijama mokėjimo operacijos autorizavimo aplinkybė, turi būti vertinama, kas ir kaip inicijavo mokėjimo operaciją ir (ar) pateikė mokėjimo paslaugų teikėjui duomenis, būtinus mokėjimo operacijai inicijuoti ir patvirtinti, taip pat turi būti analizuojamos ir visos kitos aplinkybės, pagrindžiančios arba paneigiančios vartotojo (mokėtojo) teiginį, kad valios inicijuoti ir (ar) patvirtinti ginčijamą mokėjimo operaciją (-as) vartotojas (mokėtojas) neturėjo.

Be to, sprendžiant, ar konkreti mokėjimo paslaugų vartotojo ginčijama operacija (šiuo atveju – pareiškėjos ginčijamas Mokėjimas) laikytina autorizuota, svarbu įvertinti, ar faktinės ginčijamos mokėjimo operacijos inicijavimo ir patvirtinimo aplinkybės, kurias pagrindžia ginčo byloje esantys duomenys, atitinka šalių sudarytoje sutartyje aptartą mokėjimo operacijų autorizavimo tvarką.

Iš ginčo byloje esančios pareiškėjos telefono ekrano nuotraukos, kurioje matoma trečiųjų asmenų siųsta SMS žinutė, matyti, kad banko vardu pareiškėjai išsiųstu pranešimu pareiškėja informuojama apie tariamą jos paskyros apribojimą ir pareiškėja yra raginama spausti šalia pateiktą nuorodą *seb-kontolespaslaugos.com*.

Įvertinus pirmiau aptartus duomenis, konstatuotina, kad, spausdama gautoje SMS žinutėje pateiktą nuorodą ir pagal ją atsidariusiame interneto puslapyje suvesdama prašomus pateikti duomenis, pareiškėja siekė atlikti veiksmus tariamam paskyros apribojimui panaikinti, o ne inicijuoti mokėjimo nurodymus lėšų pervedimams iš banke esančios pareiškėjos sąskaitos. Taigi, pareiškėja neketino inicijuoti ir autorizuoti Mokėjimo.

Vertinant banko teiginius, kuriais grindžiama jo pozicija dėl Mokėjimo kaip tinkamai autorizuoto, nustačius, kad jis buvo patvirtintas pareiškėjos naudojamos „Smart-ID" paskyros PIN2 kodu, be kita ko, verta atkreipti dėmesį ir į tai, kad ginčo šalių sutartinių santykių neatskiriama dalimi esančių banko Bendrųjų taisyklių sąlygose ar kituose šalių sutartinius santykius reguliuojančiuose dokumentuose nėra paaiškinama, aptariama „Smart-ID", kaip tapatybės patvirtinimo priemonės, PIN kodų suvedimo reikšmė mokėjimo operacijų vykdymo procese ir jų panaudojimo galimos pasekmės klientui. Taigi, šalių sutartinius santykius reguliuojantys dokumentai neapibrėžia, kokius veiksmus, naudodamasis „Smart-ID" programėle, banko klientas gali atlikti ir kokie veiksmai bei kokiais atvejais, naudojantis šia tapatybės patvirtinimo priemone ir suvedant jos PIN kodus, sukelia atitinkamas teisines pasekmes. Nors „Smart-ID" ir nėra banko sukurta tapatybės patvirtinimo priemonė, vis dėlto 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: naudotis banko teikiamomis paslaugomis, pateikti mokėjimo nurodymą, pasitikrinti sąskaitą, inicijuoti sutarties pakeitimus 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 jų naudojimo sąlygos ir veiksmų, atliekamų naudojantis „Smart-ID", teisinės pasekmės, pavyzdžiui, aiški PIN kodų suvedimo teisinė reikšmė.

Taigi, banko teiginio ir vertinimo, kad pati pareiškėja išreiškė savo valią ir sutikimą Mokėjimui šalių sutarta forma ir tvarka, nepatvirtina nustatytos aplinkybės. Remiantis aplinkybe, kad pareiškėja prisijungimo prie interneto banko duomenis, vėliau panaudotus siekiant inicijuoti Mokėjimą, suvedė trečiųjų asmenų sukurtame fiktyviame banko interneto banko puslapyje, sukūrusiame įspūdį, kad pareiškėjos prašoma pateikti duomenis paskyros apribojimams panaikinti, galima daryti išvadą, kad Mokėjimo inicijavimas ir patvirtinimas neatitiko pačios pareiškėjos valios, nors formaliai (pagal išorinius požymius) ir sutapo su pareiškėjos ir banko sutarta sutikimo mokėjimo operacijoms davimo forma ir tvarka.

Lietuvos banko nuomone, vertinti Mokėjimo kaip autorizuoto – atlikto esant pačios pareiškėjos sutikimui (kaip tai suprantama Mokėjimų įstatymo 29 straipsnio 1 dalies kontekste), nėra pagrindo, todėl Lietuvos bankas daro išvadą, kad Mokėjimas laikytinas neautorizuotu.

2. Dėl neautorizuotos mokėjimo operacijos pasekmių ir pareiškėjos teisės į Mokėjimo 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 dalis nustato, kad mokėtojui gali tekti dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai 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.

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 įstatymas aiškiai nustato, 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 (Mokėjimų įstatymo 37 straipsnio 3 dalis).

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).

Aplinkybių ir duomenų, kaip ir šalių ginčo dėl to, kad pareiškėja galėjo veikti nesąžiningai arba tyčia, nėra. Tai reiškia, kad, siekiant įvertinti, ar bankas pagrįstai atsisako kompensuoti pareiškėjos nuostolius, susijusius su Mokėjimo įvykdymu, ir ar galėtų pareiškėjos atžvilgiu būti taikoma Mokėjimų įstatymo 39 straipsnio 3 dalis, būtina nustatyti, ar pareiškėjos elgesys, atskleidžiant personalizuotus jai išduotų mokėjimo priemonių požymius, taip pat kiti veiksmai, dėl kurių galėjo būti įvykdytas Mokėjimas, vertintini kaip didelis pareiškėjos neatsargumas, dėl kurio visi jos reikalaujami atlyginti nuostoliai turėtų tekti pačiai pareiškėjai.

Lietuvos bankas, nagrinėdamas ginčus dėl nuostolių, susijusių su neautorizuotomis mokėjimo operacijomis, įvykusiomis dėl sukčiavimo atakų, ir spręsdamas dėl mokėjimo paslaugų teikėjo atsakomybės šiuos nuostolius atlyginti, nustačius, kad vartotojas (mokėtojas) jam teisės aktuose ir (ar) sutartyje nustatytas pareigas, susijusias su mokėjimo priemonėmis, vykdė netinkamai, elgdamasis labai neapdairiai, laikosi nuomonės, kad didelis neatsargumas yra vertinamojo pobūdžio aplinkybė. Tai reiškia, kad išvada dėl mokėtojo elgesio vertinimo kaip neatsargaus ar labai neatsargaus dėl neautorizuotos (-ų) mokėjimo operacijos (-ų) 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, šiuo atveju išvada dėl pareiškėjos, kaip mokėtojos, paprasto ar didelio neatsargumo, kaip vertinamojo pobūdžio aplinkybė, negali būti daroma izoliuotai, neįvertinus viso ginčijamo Mokėjimo įvykdymo ir su juo susijusių aplinkybių konteksto.

Bankas savo sprendimą nekompensuoti pareiškėjos nuostolių, be kita ko, grindžia pareiškėjos veiksmais, lėmusiais Mokėjimo įvykdymą, kurie, banko vertinimu, rodo pareiškėjos didelį neatsargumą vertinamomis aplinkybėmis. Banko teigimu, pareiškėja buvo labai neatsargi, nes suvedė tik jai žinomą interneto banko atpažinimo kodą ir savo asmens kodą trečiųjų asmenų sukurtoje interneto svetainėje, į kurią pateko paspaudusi SMS pranešime pateiktą nuorodą, kuri neatitinka banko interneto banko svetainės adreso ir kuri visiškai nesusijusi su banku ir jo naudojamais interneto adresais. Be to, pareiškėja, atsiradus tai padaryti raginantiems „Smart-ID" paskyros pranešimams mobiliajame telefone, suvedė ir šios savo naudojamos atpažinties priemonės PIN kodus. Bankas atkreipia dėmesį, kad pareiškėja nuspaudė trečiųjų asmenų atsiųstą nuorodą, neįsitikinusi, ar ji atitinka banko interneto banko svetainės adresą, ir nors turėjo galimybę pasitikslinti, ar SMS pranešimą tikrai atsiuntė bankas, į banką nesikreipė ir pasirinko spausti neaiškią nuorodą, o vėliau, nors turėjo galimybę suprasti, kad pati mokėjimo operacijos neinicijuoja, pasirinko suvesti savo „Smart-ID" paskyros PIN2 kodą, taip ginčijamą Mokėjimą patvirtindama.

Lietuvos bankas, siekdamas nustatyti, ar pareiškėjos elgesys vertinamų aplinkybių kontekste gali būti laikomas dideliu neatsargumu, mano, kad šiuo atveju svarbu nustatyti, kaip pareiškėja buvo įtikinta atskleisti savo mokėjimo priemonės personalizuotus saugos bei kitus duomenis tam, kad, nesant pareiškėjos valios, būtų inicijuotas ir patvirtintas Mokėjimas.

Remiantis kreipimesi pareiškėjos pateiktais paaiškinimais buvo nustatyta, kad 2022 m. birželio 18 d. pareiškėja į savo mobilųjį telefoną banko vardu gavo trečiųjų asmenų siųstą SMS pranešimą, įspėjantį ją apie paskyros apribojimą ir raginantį spausti tame pačiame SMS pranešime pateiktą nuorodą. Ginčo byloje esančiais duomenimis, pareiškėja paspaudė pranešime pateiktą nuorodą ir atsidariusiame interneto puslapyje suvedė savo interneto banko atpažinimo kodą, asmens kodą. Nors pareiškėja ir teigia neatsimenanti, ar vedė „Smart-ID" paskyros PIN1 ir PIN2 kodus, tačiau banko vidinių sistemų duomenys pagrindžia, kad tiek PIN1, tiek PIN2 kodai buvo suvesti, dėl to tretieji asmenys prisijungė prie pareiškėjos interneto banko paskyros ir suformavo Mokėjimą, kurį pareiškėja patvirtino suvesdama „Smart-ID" PIN2.

Pirmiau aptartas aplinkybes patvirtina ir pačios pareiškėjos pateikti paaiškinimai. Pareiškėja teigė, kad „2022 m. birželio 18 d. apie 15.04 val. grįžusi iš lauko į namus patikrinau telefoną ir radau sms žinutę. Žinutės siuntejo pavadinimas s.e.b. Žinutės turinys: Jūsų paskyra įšaldyta. apsilankyti seb-kontrolespaslaugos.com Žinutė atėjimo laikas 14:36 val. Paskaičiusi žinutę ją uždariau ir pasitikrinau SEB banko sąskaitą per Smart-ID. Viskas buvo tvarkoje. Atsijungusi nuo internetinės elektroninės bankininkystės vėl atsidariau sms žinutę. Nieko neįtardama paspaudžiau ant siųstos nuorodos ir vėl paprašė prisijungti prie elektroninės bankininkystės. Įvedžiau atpažinimo kodą ir savo asmens kodą. Ar dar kažką įvedžiau (pin kodą), negaliu atsakyti, nes neatsimenu. Tuo metu supratau, kad čia gali būti sukčiai ir greitai atsijungiau. Tada vėl įėjau į elektroninę bankininkystę ir pamačiau, kad iš buvusios sumos jau nuskaičiuota 1730 Eur. Iš karto skambinau į SEB banką."

Vertinant pareiškėjos veiksmų atsargumo laipsnį nagrinėjamų aplinkybių kontekste, svarbu pažymėti, kad, kaip jau minėta, ginčo šalių sutartinių santykių neatskiriama dalimi esančių banko Bendrųjų taisyklių sąlygose ar kituose šalių sutartinius santykius reguliuojančiuose dokumentuose nėra paaiškinama tapatybės patvirtinimo priemonės „Smart-ID", jos PIN kodų suvedimo reikšmė mokėjimo operacijų vykdymo procese ir jų panaudojimo galimos pasekmės klientui. Taigi, ginčo byloje nėra duomenų, kad pareiškėja būtų buvusi kokiu nors būdu tinkamai supažindinta su informacija, kokius veiksmus, naudodamasi „Smart-ID" programėle, gali atlikti ir kokie veiksmai bei kokiais atvejais, naudojantis šia tapatybės patvirtinimo priemone ir suvedant jos PIN kodus, sukelia atitinkamas teisines pasekmes sutartiniuose santykiuose su banku.

Tokia informacija plačiau atskleidžiama tik 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." Bankas, paaiškindamas klientų supažindinimo su programėlės „Smart-ID" naudojimosi ypatumais procesą, papildomai nurodė, kad „Smart-

ID" programėlės kūrėjai savo interneto svetainėje šios atpažinties priemonės naudotojams pateikia informaciją, kurioje aiškiai nurodyta „Smart-ID" PIN kodų ir veiksmų su programėle „Smart-ID" reikšmė, t. y. kad PIN1 yra naudojamas tapatybei patvirtinti, o PIN2 yra skirtas elektroniniam parašui[2].

Kita vertus, nors ginčo byloje nėra duomenų, jog būtent bankas asmeniškai supažindino pareiškėją su jos naudojamos tapatybės patvirtinimo priemonės „Smart-ID" bei jos PIN kodų suvedimo reikšme tarp šalių susiklosčiusiuose sutartiniuose santykiuose, itin svarbi aplinkybė nagrinėjamų aplinkybių kontekste yra tai, kad, pagal banko pateiktus įrodymus[3], sukčių sukurtoje svetainėje įvedus tik jai žinomus personalizuotus saugumo duomenis (atpažinimo kodą ir asmens kodą), pareiškėjos papildomai buvo prašoma patvirtinti savo tapatybę, suvedant tik pareiškėjai žinomą „Smart-ID" paskyros PIN1 kodą, ir Mokėjimą patvirtinti, t. y. patvirtinti, kad Mokėjimo informacija (suma, sąskaita, į kurią pervedamos Mokėjimo lėšos) yra teisinga. Taip pat Mokėjimo tvirtinimo metu buvo prašoma įvesti tik pareiškėjai žinomą „Smart-ID" PIN2 kodą: banko pateiktais jo informacinių sistemų žurnalo duomenimis, pareiškėjai jos naudojamoje „Smart-ID" paskyroje suvedant PIN2 kodą, kad būtų patvirtintas Mokėjimas, buvo rodomas tekstas „1 733,00 EUR i saskaita ***7690. Patvirt'-". Bankas pateikė duomenis, kad Mokėjimas buvo patvirtintas būtent suvedant pareiškėjos naudojamos atpažinties priemonės „Smart-ID" paskyros PIN2 kodą.

Taigi, remiantis ginčo byloje esančiais įrodymais, pareiškėjai, prieš suvedant savo naudojamos „Smart-ID" paskyros PIN 2 kodą, atitinkamame „Smart-ID" programėlės pranešime buvo nurodyta, kokiu tikslu pareiškėjos tai prašoma padaryti. Kaip minėta, pareiškėja teigia neatsimenanti, kad ji būtų vedusi „Smart-ID" PIN1 bei PIN2 kodus, tačiau ginčo byloje nėra jokių duomenų, kad kas nors kitas už pareiškėją būtų galėjęs tuos duomenis suvesti. Vadinasi, remiantis ginčo byloje turimais duomenimis, galima daryti labiau tikėtiną išvadą, kad pati pareiškėja suvedė „Smart-ID" PIN1 bei PIN2 kodus.

Kaip minėta, 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 Bendrųjų taisyklių 1 priedo 10 skyriuje nurodyta, 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. Be to, remiantis banko Paslaugų interneto banke teikimo sąlygų aprašo nuostatomis, klientas įsipareigoja saugoti atpažinimo priemones, nedelsdamas informuoti banką apie šių priemonių praradimą ar slaptumo pažeidimą. Jei atpažinimo priemonių praradimas susijęs su trečiųjų asmenų neteisėtais veiksmais, tai klientas privalo apie tai nedelsdamas pranešti teisėsaugos institucijoms. Už atpažinimo priemonių saugojimą ir tinkamą naudojimą, neatskleidimą tretiesiems asmenims yra atsakingas klientas. Paslaugų interneto banke teikimo sąlygų aprašas, be kita ko, nustato, kad klientas įsipareigoja laikyti paslaptyje atpažinimo kodą, slaptažodžius, PIN kodus, neužrašyti jų ant generatoriaus ar kitų kartu su juo laikomų daiktų ir jokia kita forma neatskleisti ar nepadaryti jų prieinamų tretiesiems asmenims (20.4 ir 38 punktai).

Taigi, pirmiau aptartos banko Bendrųjų taisyklių ir Paslaugų interneto banke teikimo sąlygų aprašo nuostatos, nors ir nedetalizuoja tapatybės patvirtinimo priemonės „Smart-ID" bei jos PIN kodų suvedimo teisinės reikšmės mokėjimo nurodymų įvykdyti mokėjimo operacijas inicijavimo ir patvirtinimo procese, tačiau jos aiškiai ir nedviprasmiškai nustato, kad už tapatybės patvirtinimo priemonės personalizuotų saugumo duomenų konfidencialumą yra atsakingas mokėtojas, šiuo atveju – pareiškėja.

Atsižvelgiant į tai, manytina, kad pareiškėjos elgesys būtų laikomas kaip atitinkantis mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, jei būtų nustatyta, kad pareiškėja ėmėsi adekvačių veiksmų (ar priešingai – nustačius, kad nuo tam tikrų veiksmų susilaikė) tam, kad jai banko išduotų mokėjimo priemonių personalizuotų saugumo duomenų, įgalinančių inicijuoti ir tvirtinti mokėjimus, konfidencialumas būtų tinkamai užtikrintas.

Įvertinęs ginčo byloje esančius duomenis ir ginčo nagrinėjimo metu nustatytas aplinkybes, Lietuvos bankas vis dėlto mano, kad išvados, jog pareiškėjos elgesys atitiko banko nustatytas naudojimosi mokėjimo priemonėmis sąlygas ir buvo adekvatus, pakankamas tam, kad pareiškėjai nustatytos pareigos, susijusios su mokėjimo priemonių personalizuotų saugumo duomenų konfidencialumo užtikrinimu, būtų tinkamai įvykdytos, daryti negalima.

---

[2] https://www.smart-id.com/lt/pagalba/duk/registracija/kam-yra-reikalingi-du-pin-kodai

[3] Banko informacinių sistemų žurnalo duomenys.

Visų pirma, kaip jau buvo konstatuota pirmiau, pareiškėjos ginčijamas Mokėjimas buvo patvirtintas suvedant pačios pareiškėjos naudojamos „Smart-ID" paskyros PIN2 kodą. Tokią išvadą dėl pareiškėjos elgesio kaip itin neapdairaus vertinimo aptariamų aplinkybių metu pagrindžia ir sustiprina pirmiau aptarta aplinkybė, kad „Smart-ID" pranešimas, kuriuo pareiškėjos buvo prašoma suvesti PIN2 kodą, kad būtų patvirtintas Mokėjimas, pakankamai aiškiai ir nedviprasmiškai informavo pareiškėją, kokiu tikslu jos tai padaryti prašoma, t.y. kad suvedant PIN2 kodą bus tvirtinamas atitinkamos vertės mokėjimas į konkrečią sąskaitą. Tačiau to pareiškėja nepastebėjo ir (ar) neįvertino tik dėl to, kad buvo labai neatsargi, naudodamasi savo pasirinkta atpažinties priemone.

Sprendžiant dėl pareiškėjos neatsargumo laipsnio, taip pat būtina atkreipti dėmesį į tai, kad trečiųjų asmenų pareiškėjai siųsta SMS žinutė informavo pareiškėją, kad, kaip teigia pati pareiškėja, jos „paskyra įšaldyta". Lietuvos banko nuomone, SMS žinutė su nuoroda į galimai suklastotą banko interneto banko puslapį galėjo sukurti pirminį įspūdį, kad ji siųsta banko: ji buvo siųsta banko vardu, nuorodos pavadinime naudojamas banko pavadinimas. Kita vertus, svarbu ir tai, kad SMS žinutėje pateikta nuoroda į tariamą banko interneto banko svetainę *seb-kontolespaslaugos.com.* visiškai neatitinka tikrosios banko interneto banko svetainės adreso[4] ir neturi jokių sąsajų su interneto banke teikiamomis paslaugomis ar raginimu imtis veiksmų paskyros apribojimui panaikinti.

Be to, aptariama banko vardu trečiųjų asmenų siųsta SMS žinutė, kaip matyti iš jos turinio, nepateikė jokių paaiškinimų dėl pareiškėjos lėšų „įšaldymo" (taigi, kokia pareiškėjos paskyra ir dėl kokių priežasčių apribota), kurie pagrįstų, kad pareiškėja galėjo tikėtis tokių banko veiksmų, kaip interneto banko paskyros blokavimas, ir pagrįstų protingai apdairų pareiškėjos siekį veikti žinutės nurodymais. Kaip pagrindžia banko kartu su atsiliepimu pateikti duomenys, pareiškėjai ginčijamo Mokėjimo metu suvedant PIN2 kodą, jos naudojamos „Smart-ID" paskyros lange buvo rodoma informacija, kokiu tikslu pareiškėjos buvo prašoma minėtus veiksmus atlikti, taigi, kad šį kodą pareiškėjos prašoma suvesti ne tariamam paskyros apribojimui panaikinti.

Manytina, kad šios aplinkybės, kurios vidutiniškai apdairų ir rūpestingą vartotoją būtų privertusios sudvejoti dėl atliekamų veiksmų ir pateiktų prašymų pagrįstumo, pareiškėjai galėjo nesukelti jokių abejonių tik dėl to, kad vertinamų aplinkybių metu pareiškėja buvo itin neatidi – prieš suvesdama savo naudojamos „Smart-ID" paskyros PIN2 kodą, pareiškėja, tikėtina, neperskaitė ar neįvertino atitinkamo „Smart-ID" programėlės pranešimo teksto, informavusio pareiškėją, kokiu tikslu jos prašoma suvesti šį kodą. Pareiškėja ne tik paspaudė nuorodą į suklastotą banko interneto banko svetainę, atskleisdama ten savo mokėjimo priemonių personalizuotus saugumo duomenis, bet ir neperskaičiusi ar neįvertinusi „Smart-ID" programėlės pranešimų teksto, aiškiai nurodžiusio prašomų atlikti veiksmų tikslą, suvedė „Smart-ID" paskyros PIN2 kodą.

Aptariamų aplinkybių kontekste įvertintina ir tai, kad, banko pateiktais duomenimis, banko interneto banko paslaugomis su mobiliajame telefone susikurta „Smart-ID" paskyra pareiškėja naudojasi dar nuo 2018 m., tad tikrasis banko interneto banko svetainės adresas, kaip ir naudojimosi pačia „Smart-ID" programėle esminiai ypatumai (pavyzdžiui, kokiu tikslu gali būti prašoma suvesti „Smart-ID" PIN2 kodą ir kad šios programėlės pranešimuose, prašančiuose suvesti PIN kodus, įprastai rodoma ir (ar) gali būti rodoma informacija, kokiu tikslu prašoma tai atlikti) pareiškėjai turėjo būti žinomi.

Be to, bankas kartu su atsiliepimu Lietuvos bankui pateikė duomenis, kad yra siuntęs (pvz., 2022 m. gegužės 23 d.) įspėjamuosius pranešimus į pareiškėjos interneto banko paskyrą apie sukčių atakas su raginimu nespausti jokių siunčiamų aktyvių nuorodų. Bankas taip pat nurodo nuolat informuojantis savo klientus apie su sukčiavimu susijusias rizikas savo interneto svetainėje[5].

Kaip minėta pirmiau, išvada dėl mokėtojo elgesio vertinimo kaip neatsargaus ar labai neatsargaus dėl neautorizuotos mokėjimo operacijos 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

[4] https://www.seb.lt/privatiems/kasdiene-bankininkyste/nuotolines-paslaugos/interneto-bankas; https://e.seb.lt/web/ipank.p?lang=lit.

[5] Nusikaltėliai internete tobulėja. Ką gali nuveikti turėdami Jūsų duomenis? | SEB ; Telefoniniai sukčiai apsimeta ir kurjeriais: kada verta sunerimti? | SEB ; Nusikaltėliai internete tobulėja. Ką gali nuveikti turėdami Jūsų duomenis? | SEB ; https://www.seb.lt/infobankas/naujienos/gresme-savo-pinigams-galime-nesiotis-kiseneje-kaip-nuo-jos-apsisaugoti .

mokėjimo operacijos įvykdymo aplinkybės. Vis dėlto šiuo atveju nustatytos ir pirmiau analizuotos aplinkybės, susijusios tiek su pačios sukčiavimo atakos pobūdžiu, tiek su banko veiksmais, o svarbiausia – susijusios su pačios pareiškėjos veiksmais, ir būtent šių aplinkybių visuma, nesudaro pagrindo vertinti pareiškėjos elgesio tik kaip neatsargaus.

Pareiškėja kritiškai neįvertino gautos SMS žinutės turinio, paspaudė joje pateiktą nuorodą ir suklastotoje banko interneto banko svetainėje suvedė personalizuotus saugumo duomenis ir nedvejojusi suvedė savo „Smart-ID" paskyros PIN2 kodą tik todėl, kad nebuvo atsargi ir rūpestinga, kiek akivaizdžiai buvo būtina vertinamomis aplinkybėmis. Taigi, pareiškėja ne tik netinkamai vykdė jai, kaip mokėtojai, Mokėjimų įstatyme nustatytas pareigas, susijusias su jai išduotomis mokėjimo priemonėmis ir jų personalizuotais saugumo duomenimis, bet ir darė tai elgdamasi labai neatsargiai.

Tai reiškia, kad pareiškėjos elgesys vertinamomis aplinkybėmis nebuvo toks, koks akivaizdžiai buvo būtinas, ir tai šiuo atveju lėmė, kad tretieji asmenys įgijo galimybę pareiškėjos vardu inicijuoti Mokėjimą, kurį suvesdama savo „Smart-ID" paskyros PIN2 kodą patvirtino pati pareiškėja, prieš tai neperskaičiusi ir (ar) neįvertinusi „Smart-ID" programėlės pranešimo, taigi, i nesudvejojusi dėl tokio prašymo naudoti savo atpažinties priemonę pagrįstumo.

Konstatavus, kad pareiškėja, nesilaikydama jai, kaip mokėtojai, Mokėjimų įstatyme ir sutartyje su banku nustatytų pareigų, susijusių su jai išduotomis mokėjimo priemonėmis, elgėsi labai neatsargiai, kartu darytina išvada, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, nustatančią, kad tokiu atveju mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai. Dėl šios priežasties, Lietuvos banko vertinimu, bankas neturi pareigos grąžinti (kompensuoti) pareiškėjai neautorizuoto Mokėjimo lėšų.

Įvertinus visa tai, kas išdėstyta pirmiau, ir nustačius, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, darytina išvada, kad pareiškėjos bankui keliamas reikalavimas grąžinti ir (ar) kompensuoti pareiškėjai Mokėjimo 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. 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