LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

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

2022 m. lapkričio 16 d. Nr. 429-581
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. gegužės 22 d. 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 keturis mokėjimus: 999 Eur vertės mokėjimas, du 331 Eur vertės mokėjimai ir 889 Eur vertės mokėjimas, kurie buvo patvirtinti suvedant pareiškėjos naudojamos atpažinties priemonės „Smart-ID" paskyros PIN2 kodą (toliau – Mokėjimai).

2022 m. gegužės 22 d. 19:23 val. pareiškėja kreipėsi į banką telefonu, norėdama pranešti apie sukčiavimo atvejį. Telefoninio pokalbio metu banko darbuotoja užblokavo pareiškėjos interneto banko paskyrą ir rekomendavo kreiptis į teisėsaugos institucijas.

2022 m. gegužės 23 d. bankas kreipėsi į lėšų gavėjo mokėjimo paslaugų teikėją *Verse Payments Lithuania UAB* dėl Mokėjimų sumų grąžinimo, tačiau lėšų gavėjo mokėjimo paslaugų teikėjas nepateikė atsakymo bankui dėl prašymo grąžinti Mokėjimų lėšas. Apie tai bankas informavo pareiškėją 2022 m. birželio 13 d. pranešimu pareiškėjos interneto banko paskyroje.

Pareiškėja, ginčydama banko sprendimą nekompensuoti jos nuostolių dėl įvykdytų Mokėjimų, kreipėsi į Lietuvos banką dėl ginčo nagrinėjimo. Kreipimesi pareiškėja teigia, kad Mokėjimai buvo inicijuoti ir įvykdyti trečiųjų asmenų, šiems neteisėtai pasisavinus pareiškėjos mokėjimo priemonių personalizuotus saugumo duomenis, todėl Mokėjimai laikytini neautorizuotais. Pareiškėja mano, kad bankas nesiėmė reikiamų veiksmų tam, kad apsaugotų pareiškėjos banko sąskaitose esančių lėšų saugumą nuo trečiųjų asmenų neteisėtos veiklos (sukčiavimo atakos). Be to, pareiškėja pažymi, kad, įvykus sukčiavimo atakai, ji iš karto, t. y. 17:25 val., paskambino į banką, siekdama atšaukti mokėjimus, tačiau į jos skambutį tuomet nebuvo atsiliepta. Pareiškėjos teigimu, po daugybės skambučių jai pavyko prisiskambinti bankui tik tos pačios dienos 19:20 val. Atsižvelgdama į tai, pareiškėja mano, kad jeigu bankas į jos skambučius būtų atsiliepęs greičiau nei per 2 valandas, jai būtų buvusi didesnė galimybė atgauti ginčijamų Mokėjimų lėšas. Kreipimesi pareiškėja prašo rekomenduoti bankui kompensuoti pareiškėjai jos ginčijamų Mokėjimų sumas.

Bankas nesutinka tenkinti pareiškėjos reikalavimo. Bankas mano, kad pareiškėja elgėsi itin neapdairiai: paspaudė neaiškią nuorodą, suvedė savo interneto banko ID, asmens kodą ir savo mobiliajame įrenginyje savo atliekamus veiksmus patvirtino suvesdama tik pareiškėjai žinomus „Smart-ID" paskyros PIN1 ir PIN2 kodus, dėl to tretieji asmenys galėjo ne tik pareiškėjos vardu inicijuoti Mokėjimus, bet ir ginčijami Mokėjimai buvo tinkamai patvirtinti.

Atsiliepime pažymima, kad operacijoms tvirtinti bankas taiko papildomą kliento ir jo operacijų autentifikavimą, taip siekiama suteikti galimybę klientui įsitikinti inicijuojamos operacijos teisėtumu. Klientams įvykdžius visas būtinas banko ir kliento sutartas sąlygas, padedančias tinkamai identifikuoti kliento inicijuotą operaciją, bankas įsipareigoja tokias operacijas įvykdyti. Bankas nurodo, kad Mokėjimų vykdymo metu banko sistemos veikė

saugiai, jokių sutrikimų užfiksuota nebuvo. Banko vertinimu, Mokėjimo įvykdymą lėmė tai, kad pareiškėja paspaudė nuorodą, kuri nuvedė į sukčių sukurtą interneto puslapį, suvedė tik pareiškėjai žinomus personalizuotus saugumo duomenis, o vėliau ir savo naudojamos atpažinties priemonės („Smart-ID" paskyros) PIN kodus, taip suteikdama galimybę sukčiams inicijuoti ir atlikti Mokėjimus. Bankas teigia dedantis visas pastangas ir vykdo visus reikalavimus, kad užtikrintų klientų lėšų saugumą, tačiau neturi galimybės kontroliuoti klientų neatsargių veiksmų, kurie nėra ir negali būti banko kontroliuojami. Įvertinęs aplinkybių visumą ir teisinį reglamentavimą, bankas mano, kad neturi pareigos pareiškėjai kompensuoti nuostolių, patirtų dėl įvykdytų Mokėjimų.

K o n s t a t u o j a m a:

Vadovaujantis Lietuvos banko valdybos 2012 m. sausio 26 d. nutarimu Nr. 03-23 patvirtintų Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių (toliau – Taisyklės) 45 punktu, vartojimo ginčai Lietuvos banke nagrinėjami laikantis rungimosi, ginčų nagrinėjimo operatyvumo, koncentracijos, ekonomiškumo ir bendradarbiavimo principų. Vartotojas ir finansų rinkos dalyvis privalo įrodyti tas aplinkybes, kuriomis remiasi kaip savo reikalavimų arba atsikirtimų pagrindu, išskyrus atvejus, kai remiamasi aplinkybėmis, kurių nereikia įrodinėti. Lietuvos bankas ginčo nagrinėjimo proceso metu neatlieka Lietuvos Respublikos Lietuvos banko įstatymo 42^1 straipsnyje reglamentuojamų patikrinimų, skirtų faktinėms aplinkybėms, susijusioms su Lietuvos banko priežiūrimo finansų rinkos dalyvio galimai padarytu 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 ir (ar) kompensuoti pareiškėjai jos ginčijamų Mokėjimų, įvykdytų dėl trečiųjų asmenų surengtos sukčiavimo atakos, sumas. Pareiškėja mano, kad bankas nesiėmė reikiamų veiksmų tam, kad apsaugotų jos banko sąskaitoje esančias lėšas, o įvykus neautorizuotiems Mokėjimams – kad padėtų pareiškėjai atgauti jos ginčijamų Mokėjimų sumas, todėl bankas turėtų kompensuoti pareiškėjai su Mokėjimų įvykdymu susijusius nuostolius (Mokėjimų sumą). Bankas teigia, kad tretieji asmenys įgijo sąlygas inicijuoti Mokėjimus tik dėl to, kad pareiškėja dėl didelio neatsargumo atskleidė savo mokėjimo priemonių personalizuotus saugumo duomenis tretiesiems asmenims ir Mokėjimus patvirtino suvesdama savo naudojamos „Smart-ID" paskyros PIN2 kodą, todėl Mokėjimų 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) Mokėjimai laikytini autorizuotais; 2) bankas turėjo (turi) pareigą grąžinti (kompensuoti) pareiškėjai Mokėjimų sumą; 3) bankas tinkamai reagavo į pareiškėjos bandymą pranešti apie neteisėtą jos mokėjimo priemonės panaudojimą ir pagrįstai įvykdė ginčijamus Mokėjimus; 4) pareiškėjos nuostolius galėjo lemti tai, kad bankas nesiėmė veiksmų ir priemonių užtikrinti pareiškėjos banko sąskaitose esančių lėšų saugumą.*

1. Dėl ginčijamų Mokėjimų 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".

Darydamas išvadą, kad Mokėjimams atlikti buvo tinkamai, taigi, šalių sutarta tvarka, išreikštas pareiškėjos sutikimas, bankas remiasi banko vidinės sistemos duomenimis, kurie patvirtina šalių (taigi, tiek pareiškėjos, tiek banko) neginčijamą aplinkybę, kad Mokėjimams įvykdyti buvo panaudoti pareiškėjos interneto banko prisijungimo duomenys – interneto banko naudotojo ID kodas ir pareiškėjos vardu išduotos atpažinimo priemonės „Smart-ID" PIN1 ir PIN2 kodai. Atsižvelgdamas į tai, kad Mokėjimai buvo patvirtinti šalių sutartu būdu, taikant griežtą kliento (šiuo atveju – pareiškėjos) tapatybės nustatymo procesą, bankas mano, kad nėra pagrindo laikyti Mokėjimų neautorizuotais.

Kaip matyti iš banko paaiškinimų, darydamas išvadą, kad Mokėjimai buvo tinkamai pareiškėjos patvirtinti ir laikytini autorizuotais, bankas papildomai nevertino Mokėjimų inicijavimo ir patvirtinimo aplinkybių, kas perdavė lėšų gavėjui ir (arba) jo mokėjimo paslaugų teikėjui duomenis, kurių pagrindu buvo inicijuoti Mokėjimai, t. y. ar šiuos duomenis tiesiogiai pateikė pati pareiškėja, ar iš pareiškėjos šiuos duomenis neteisėtai išvilioję tretieji asmenys. Tad nors bankas kartu su atsiliepimu pateikė jo vidaus sistemose užfiksuotus duomenis, pagrindžiančius, kad, prieš įvykdant Mokėjimus, siekiant prisijungti prie pareiškėjos interneto banko paskyros, buvo panaudoti interneto banko prisijungimo duomenys, o patys Mokėjimai papildomai patvirtinti pagal griežtą tapatybės nustatymo procesą, t. y. suvedus tik pareiškėjai žinomus jos naudojamos tapatybės patvirtinimo priemonės „Smart-ID" paskyros PIN1 ir PIN2 kodus, tačiau vien šie duomenys, Lietuvos banko vertinimu, savaime dar neįrodo, kad Mokėjimai iš tiesų atlikti gavus pareiškėjos sutikimą (pareiškėjos valia).

Vadinasi, bankas, siekdamas pagrįsti teiginį, kad Mokėjimams atlikti buvo tinkamai, t. y. šalių sutartu būdu, išreikštas pareiškėjos sutikimas, remiasi pirmiau aptartomis banko Bendrųjų taisyklių nuostatomis. Vis dėlto būtina pažymėti, kad 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). Nagrinėjant ginčą 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 būtų tariamai 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 lėšų pervedimo operacijai, 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 mokėjimo operacijai davimo formą, negali būti laikomi tinkamu mokėtojo sutikimu įvykdyti 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, ar Mokėjimai laikytini autorizuotais, tačiau turi būti vertinami konkretūs pareiškėjos atlikti veiksmai ir tai, kaip jie atitinka su banku sutartos sutikimo atlikti mokėjimo operaciją formos 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, kad 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. Vis dėlto Lietuvos bankas pažymi, kad valia yra esminis kiekvieno sandorio, kaip teisinio veiksmo, kuriuo siekiama sukurti tam tikras teises ir pareigas, elementas[1]. Tai reiškia, kad, nesant mokėtojo valios inicijuoti lėšų pervedimo operaciją, 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 negalėjo žinoti, kad jo vardu yra pateikiamas mokėjimo nurodymas pervesti lėšas.

Tad 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 (šiuo atveju – pareiškėjos) valios išraiškos forma vertintina ne tik per 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 kokiu būdu inicijavo ir (ar) pateikė mokėjimo paslaugų teikėjui duomenis, būtinus mokėjimo operacijai inicijuoti ir patvirtinti, taip pat turi būti analizuojamos ir visos kitos ginčo nagrinėjimo metu nustatytos 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 ginčijami Mokėjimai) 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.

Pareiškėja, pagrįsdama teiginį, kad nesiekė inicijuoti ir neautorizavo Mokėjimų, pateikė savo telefono ekrano su gauta žinute nuotrauką, kuri patvirtina pareiškėjos teiginius: iš minėtos nuotraukos matyti, kad banko vardu pareiškėjai išsiųsta SMS žinute tretieji asmenys informuoja pareiškėją apie tariamą jos paskyros apribojimą ir pareiškėja yra raginama spausti šalia pateiktą nuorodą *seb-acc-lt-paslaugos.com*.

Įvertinus pirmiau aptartus duomenis, konstatuotina, kad, spausdama gautoje SMS žinutėje pateiktą nuorodą ir pagal ją atsidariusiame interneto puslapyje suvesdama prašomus duomenis (mokėjimo priemonių personalizuotus saugumo duomenis), pareiškėja siekė tariamai atblokuoti paskyrą, o ne inicijuoti mokėjimo nurodymus lėšų pervedimams iš banke esančių pareiškėjos sąskaitų. Taigi, ginčo byloje esantys duomenys suponuoja, kad pareiškėja valios inicijuoti Mokėjimų įvykdymą, taip pat ir jų autorizuoti, neturėjo.

Vadinasi, ginčo byloje esantys įrodymai, tarp jų ir pirmiau aptarti įrodymai dėl Mokėjimų inicijavimo ir įvykdymo aplinkybių, kurių nepaneigė banko paaiškinimai ir pateikti vidinės sistemos duomenys, kad Mokėjimams patvirtinti panaudoti pareiškėjos prisijungimo prie interneto banko duomenys ir suvesti pareiškėjos naudojamos atpažinties priemonės „Smart-ID" PIN kodai, Lietuvos banko vertinimu, leidžia daryti išvadą, kad trečiųjų asmenų sukurtoje aplinkoje pareiškėjai nebuvo rodoma tikrovę atitinkanti informacija apie inicijuotus Mokėjimus, ir tai galėjo suklaidinti pareiškėją dėl toliau atliekamų veiksmų esmės ir pobūdžio. Tai reiškia, kad duomenų, jog ginčo šalių susitarime aptarti sutikimo atlikti mokėjimo operaciją formalūs išoriniai veiksmai atitiko pareiškėjos valią, kitaip tariant, duomenų, kad pareiškėja, žinojo, suprato ir pati išreiškė savo valią autorizuoti Mokėjimus šalių sutarta tvarka, ginčo byloje nėra.

Vertinant banko teiginius, kuriais grindžiama jo pozicija dėl Mokėjimų kaip tinkamai autorizuotų, nustačius, kad šie mokėjimai buvo patvirtinti pareiškėjos naudojamos „Smart-ID"

[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).

paskyros PIN kodais, 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, t. y. 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 jos naudojimo sąlygos ir veiksmų, atliekamų su „Smart-ID", teisinės pasekmės, pavyzdžiui, aiški PIN kodų suvedimo teisinė reikšmė.

Taigi, banko teiginio ir vertinimo, kad pati pareiškėja išreiškė savo valią ir sutikimą, kad Mokėjimai būtų atlikti, šalių sutarta forma ir tvarka, nepatvirtina ginčo nagrinėjimo metu nustatytos aplinkybės. Todėl, remiantis aplinkybe, kad pareiškėjos prisijungimo prie interneto banko duomenys, panaudoti siekiant inicijuoti Mokėjimus, buvo suvesti trečiųjų asmenų sukurtame fiktyviame banko interneto banko puslapyje, sukūrusiame įspūdį, kad pareiškėjos prašoma pateikti duomenis paskyrai atblokuoti, galima daryti išvadą, kad Mokėjimų inicijavimas ir patvirtinimas neatitiko pačios pareiškėjos valios, nors formaliai (pagal išorinius požymius) ir sutapo su pareiškėjos ir banko sutarta sutikimo atlikti mokėjimo operacijas davimo forma ir tvarka. Lietuvos banko nuomone, vertinti Mokėjimus kaip autorizuotus – atliktus esant pačios pareiškėjos sutikimui (kaip tai suprantama Mokėjimų įstatymo 29 straipsnio 1 dalies kontekste), nėra pagrindo, todėl šio ginčo nagrinėjimo metu Lietuvos bankas daro išvadą, kad Mokėjimai laikytini neautorizuotais.

2. Dėl neautorizuotos mokėjimo operacijos pasekmių ir pareiškėjos teisės į Mokėjimų sumų 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 Mokėjimų 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 įvykdyti Mokėjimai, 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 ginčijamų Mokėjimų įvykdymo ir su jais susijusių aplinkybių konteksto.

Bankas savo sprendimą nekompensuoti pareiškėjos nuostolių, be kita ko, grindžia pareiškėjos veiksmais, lėmusiais Mokėjimų įvykdymą, kurie, banko vertinimu, rodo pareiškėjos didelį neatsargumą. Bankas mano, kad 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 jokių mokėjimo operacijų neinicijuoja, pasirinko kiekvieną kartą (t.y. kiekvieno iš inicijuotų Mokėjimų atveju) suvesti savo „Smart-ID" paskyros PIN2 kodą, taip juos 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 inicijuoti ir patvirtinti Mokėjimai.

Remiantis kreipimesi pareiškėjos pateiktais paaiškinimais buvo nustatyta, kad 2022 m. gegužės 22 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. Šalių neginčijamomis aplinkybėmis ir ginčo byloje esančiais duomenimis, pareiškėja paspaudė pranešime pateiktą nuorodą ir atsidariusiame interneto puslapyje suvedė savo interneto banko atpažinimo kodą, asmens kodą ir savo mobiliajame įrenginyje į savo „Smart-ID" paskyrą, gavusi patvirtinimo užklausas, suvedė tik jai žinomus

„Smart-ID“ paskyros PIN1 kodą (kai šis kodas buvo suvestas, tretieji asmenys prisijungė prie pareiškėjos interneto banko paskyros) ir „Smart-ID“ paskyros PIN2 kodą. Kiekvieną kartą (t. y. kiekvieno iš Mokėjimų atveju) suvesdama šį kodą pareiškėja patvirtino trečiųjų asmenų pareiškėjos vardu suformuotus Mokėjimus.

Ginčo nagrinėjimo metu Lietuvos bankas paprašė pareiškėjos plačiau paaiškinti aplinkybes, susijusias su Mokėjimo įvykdymu ir, esant galimybei, pateikti trečiųjų asmenų siųstos SMS žinutės bei suklastotos banko interneto banko svetainės ekrano vaizdus, kurie padėtų suprasti ir geriau įvertinti tiek sukčiavimo atakos pobūdį, tiek ir pačios pareiškėjos veiksmus (elgesį) jos ginčijamų Mokėjimų inicijavimo ir įvykdymo metu.

Papildomuose paaiškinimuose pareiškėja nurodė, kad, paspaudus trečiųjų asmenų siųstoje SMS žinutėje pateiktą nuorodą, jai nekilo įtarimų, kad pagal nuorodą atsidariusi interneto svetainė galėtų būti suklastota banko interneto banko svetainė, nes ji atrodė taip pat, kaip ir tikra banko interneto banko svetainė. Pareiškėjos teigimu, „<...> nuoroda prasidėjo seb.lt/ <...>. Viršuje buvo mėlyna ekrano juosta, joje SEB žalias logo, o baltame šone parašyta „Prisijungimas“, „"Pasirinkite identifikavimo priemonę“. Tekstas, šriftas, spalvos ir išdėstymas nesukėlė jokių abejonių – svetainė vizualiai atrodė įprastai. Pasirinkus Smart-ID identifikavimo priemonę atsirado pranešimas „patvirtinti prisijungimą prie paskyros“, vėliau buvo eilutė smulkiu šriftu su mano sąskaitos numeriu ir užrašas „patvirtinti“. Įvedžiau savo PIN2 kodą. Po kurio laiko vėl atsirado užrašas ekrano viršuje „patvirtinti prisijungimą prie paskyros“ ir eilutė smulkiu šriftu su mano kitos sąskaitos numeriu ir vėl „patvirtinti“. Šiuo momentu, pagalvojau kad reikia kelis kartus patvirtinti dėl to, kad turiu kelias sąskaitas. Aš nepamenu arba nepastebėjau (nes šriftas buvo smulkus), kad tame užraše būtų informacija apie mokėjimo sumą ir jo gavėją. Aš ne kartą vykdžiau mokėjimus naudojant Smart-ID ir žinau, kad atliekant mokėjimą pranešimo tekstas būna aiškiai matomas ekrane, kartu su mokėjimo suma ir gavėju. Šiuo atveju vizualus vaizdas buvo kitoks. Galiausiai, ekrane pasirodė pranešimas „operacija baigta“.“

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 kokiu nors būdu tinkamai supažindinta su informacija, kokius veiksmus, naudodamasi „Smart-ID“ programėle, ji 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 būtų asmeniškai supažindinęs 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], pareiškėjai, sukčių sukurtoje svetainėje įvedus tik jai žinomus personalizuotus saugumo duomenis (atpažinimo kodą ir asmens kodą), jos papildomai buvo prašoma patvirtinti savo tapatybę, suvedant tik pareiškėjai žinomą „Smart-ID“ paskyros PIN1 kodą, ir Mokėjimus patvirtinti, t. y. patvirtinti, kad kiekvieno iš inicijuotų Mokėjimų informacija (suma, sąskaita, į kurią pervedamos Mokėjimų lėšos) yra teisinga, taip pat tvirtinant kiekvieną iš Mokėjimų buvo prašoma įvesti tik pareiškėjai žinomą „Smart-ID“ PIN2 kodą. Banko pateiktais jo informacinių

[2] https://www.smart-id.com/lt/pagalba/duk/registracija/kam-yra-reikalingi-du-pin-kodai
[3] Banko informacinių sistemų žurnalo duomenys.

sistemų žurnalo duomenimis, pareiškėjai savo naudojamoje „Smart-ID" paskyroje suvedant PIN2 kodą tvirtinant kiekvieną Mokėjimą buvo rodomi tekstai „999,00 EUR i saskaita ***3474. Patvirtin", „3 331,00 EUR i saskaita ***2158. Patvirtin", „3 331,00 EUR i saskaita ***3474. Patvirtin" ir atitinkamai „889,00 EUR i saskaita ***3474. Patvirtin". Bankas pateikė duomenis, kad visi Mokėjimai buvo patvirtinti suvedant būtent pareiškėjos naudojamos atpažinties priemonės „Smart-ID" paskyros PIN2 kodą.

Tai reiškia, kad nors pareiškėja teigia neprisimenanti, kad suvesdama PIN2 kodą „Smart-ID" programėlės languose būtų mačiusi mokėjimo operacijos sumą ir gavėją (sąskaitos numerį), kurio naudai atliekamas mokėjimas, vis dėlto, remiantis ginčo byloje esančiais įrodymais, pareiškėjai, prieš suvedant savo naudojamos „Smart-ID" paskyros PIN 2 kodą, kiekvieno iš Mokėjimų tvirtinimo metu atitinkamuose „Smart-ID" programėlės pranešimuose buvo nurodyta, kokiu tikslu pareiškėjos tai prašoma padaryti (t. y. kiekvieną kartą suvesti „Smart-ID" paskyros PIN 2 kodą).

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 papunktis ir 38 punktas).

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.

Visų pirma, kaip jau buvo konstatuota pirmiau, ginčo byloje turimais įrodymais, visi pareiškėjos ginčijami Mokėjimai buvo patvirtinti 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" pranešimai, kuriais pareiškėjos buvo prašoma suvesti PIN2 kodą kiekvieno iš Mokėjimų tvirtinimo atveju, pakankamai aiškiai ir nedviprasmiškai informavo pareiškėją, kokiu tikslu jos tai padaryti prašoma, t. y. kad suvedant PIN2 kodą bus tvirtinami atitinkamos vertės mokėjimai 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 pareiškėjui siųsta SMS žinutė informavo pareiškėją, kad, kaip teigia pati pareiškėja, jos „paskyra blokuota". Iš pareiškėjos Lietuvos bankui pateiktos trečiųjų asmenų banko vardu siųstos SMS žinutės ekrano vaizdo galima teigti, kad ši SMS žinutė su nuoroda į galimai suklastotą banko interneto banko puslapį galėjo sukurti pirminį įspūdį, kad ji siųsta

banko (buvo siųsta banko vardu). Kita vertus, būtina pastebėti, kad aptariama SMS žinutė yra parašyta su klaidomis („seb:Js paskyra buvo apribota. apsilankykite seb-acc-lt-paslaugos.com"), tačiau į tai pareiškėja, prieš paspausdama joje pateiktą nuorodą ir suvesdama savo mokėjimo priemonių personalizuotus saugumo duomenis, neatkreipė dėmesio, tikėtina, dėl skubėjimo ir nepakankamo atidumo.

Be to, aptariama banko vardu trečiųjų asmenų siųsta SMS žinutė, kaip matyti iš jos turinio, nepateikė jokių paaiškinimų dėl pareiškėjos „paskyros apribojimo" (taigi, kokia pareiškėjos paskyra ir dėl kokių priežasčių apribota), kurie pagrįstų tai, kad pareiškėja galėjo tikėtis tokių banko veiksmų, kaip interneto banko paskyros blokavimas, ir kad tai pagrįstų protingai apdairų pareiškėjos siekį veikti vykdant žinutės nurodymus. Remiantis pareiškėjos kreipimesi pateiktais paaiškinimais, iš trečiųjų asmenų gauta SMS žinutė jai nesukėlė įtarimų ir ji paspaudė joje pateiktą nuorodą ir dėl to, kad bankas 2022 m. gegužės 20 d. buvo informavęs pareiškėją, kad savaitgalį – 2022 m. gegužės 20–22 d., bus atliekami planiniai informacinių sistemų profilaktikos darbai. Todėl pareiškėja, gavusi trečiųjų asmenų banko vardu siųstą SMS žinutę, pagalvojo, kaip nurodoma kreipimesi, kad „įvyko techninis prisijungimo sistemos atnaujinimas, todėl reikėjo pareiti patvirtinimą."

Vis dėlto, banko pateiktais duomenimis, 2022 m. gegužės 20 d. bankas interneto banko pranešimais informavo klientus apie savaitgalį vyksiančius planinius profilaktikos darbus, kurių metu gali pasitaikyti trumpalaikių (iki 15 min.) sutrikimų naudojantis interneto banku ir mobiliąja programėle ir trumpalaikių (iki 1–2 min.) sutrikimų naudojantis mokėjimo kortelėmis. Atsiliepime nurodoma, kad šiame banko pranešime apie planinius profilaktikos darbus klientams nebuvo nurodyta, kad dėl šių profilaktinių darbų gali reikėti prisijungti prie asmeninės interneto banko paskyros ar tvirtinti operacijas. Paaiškinimų, kodėl, bankui atlikus informacinių sistemų profilaktikos darbus, pareiškėja būtų banko informuota apie jos paskyros apribojimą ir dėl ko ji turėtų ne tik prisijungti prie savo interneto banko, suvesdama savo asmens kodą, bet ir net keturis kartus suvesti naudojamos atpažinties priemonės „Smart-ID" PIN2 kodą, pareiškėja nepateikė.

Aptariamų aplinkybių kontekste įvertintina ir tai, kad, banko pateiktais duomenimis, banko interneto banko paslaugomis su mobiliajame telefone susikurta „Smart-ID" paskyra pareiškėja naudojasi nuo 2021 m. liepos mėn., 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. Kaip pagrindžia banko kartu su atsiliepimu pateikti duomenys, pareiškėjai kiekvieno iš ginčijamų Mokėjimų metu suvedant PIN2 kodą, jai jos naudojamos „Smart-ID" paskyros lange buvo rodoma informacija, kokiu tikslu pareiškėjos buvo prašomos minėtus veiksmus atlikti.

Be to, bankas kartu su atsiliepimu Lietuvos bankui pateikė duomenis, kad yra siuntęs (pvz., 2021 m. spalio 21 d.) įspėjamuosius pranešimus į pareiškėjos interneto banko paskyrą bei SMS žinutes 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[4]. Manytina, kad šios aplinkybės, kurios vidutiniškai apdairų ir rūpestingą vartotoją būtų privertę sudvejoti atliekamų veiksmų ir pateiktų prašymų pagrįstumu, pareiškėjai galėjo nesukelti jokių abejonių tik dėl to, kad vertinamų aplinkybių metu pareiškėja buvo itin neatidi.

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 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, suklastotoje banko interneto banko svetainėje suvedė personalizuotus saugumo duomenis ir nedvejojusi suvedė

[4] 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 .

savo „Smart-ID" paskyros PIN2 kodą 4 kartus 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 Mokėjimus, kuriuos atlikti patvirtinimas duotas pačiai pareiškėjai savo „Smart-ID" paskyroje suvedus paskyros PIN2 kodą, prieš tai neperskaičius ir (ar) neįvertinus „Smart-ID" programėlės pranešimų turinio prasmės, taigi, neįvertinus ir nesudvejojus 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.

3. Dėl banko, kaip mokėjimo paslaugų teikėjo, veiksmų, sužinojus apie neautorizuotą mokėjimo operaciją, pagrįstumo

Pareiškėja kreipimesi, be kita ko, teigia, kad supratusi, jog galėjo būti apgauta sukčių, bandė prisiskambinti į banką, t. y. pareiškėja nurodė pirmą kartą paskambinusi bankui 2022 m. gegužės 22 d. 17:25 val., tačiau tuomet niekas į jos skambutį neatsiliepė. Pareiškėjos teigimu, tik po daugybės skambučių jai pavyko prisiskambinti į banką tos pačios dienos vakare 19:20 val. Pareiškėja mano, kad jei bankas būtų atsiliepęs į jo skambučius anksčiau nei per dvi valandas, Mokėjimų sumų grąžinimo tikimybė būtų buvusi didesnė.

Mokėjimų įstatymo 34 straipsnio 1 dalies 2 punkte nurodyta, kad mokėtojas, sužinojęs apie mokėjimo priemonės praradimą, vagystę arba neteisėtą pasisavinimą ar neautorizuotą jos naudojimą, nedelsdamas apie tai turi pranešti mokėjimo paslaugų teikėjui arba jo nurodytam subjektui. Vadovaujantis Mokėjimų įstatymo 39 straipsnio 5 dalies nuostatomis, „mokėtojas neturi patirti jokių nuostolių dėl prarastos, pavogtos ar neteisėtai pasisavintos mokėjimo priemonės po to, kai pateikia šio įstatymo 34 straipsnio 1 dalies 2 punkte nurodytą pranešimą, išskyrus atvejus, kai jis veikė nesąžiningai."

Ginčo byloje nustatytais duomenimis, visi pareiškėjos ginčijami Mokėjimai buvo įvykdyti ir iš pareiškėjos sąskaitos nurašyti 2022 m. gegužės 22 d. 17:18:11 val., 17:19:31 val., 17:20:32 val. ir atitinkamai 17:21:28 val. Taigi, iki pirmojo pareiškėjos bandymo prisiskambinti bankui, banko informacinių sistemų duomenimis, skambinta 17:25:11 val. Ginčo bylos duomenimis, Mokėjimai iš pareiškėjos sąskaitos banke buvo įvykdyti dar iki pareiškėjos skambučio į banką ir pranešimo apie mokėjimo priemonės paradimą bei neautorizuotą jos panaudojimą. Tai reiškia, kad pareiškėja į banką dėl ginčijamų Mokėjimų paskambino jau po to, kai sutikimas atlikti minėtas mokėjimo operacijas buvo duotas ir pačios neautorizuotos bei pareiškėjos ginčijamos mokėjimo operacijos (t. y. Mokėjimai) jau buvo įvykdytos.

Lietuvos bankas neturi pakankamai duomenų, kurie patvirtintų ar paneigtų pareiškėjos teiginį, kad jei ji būtų prisiskambinusi į banką anksčiau, tikimybė atgauti Mokėjimų lėšas būtų buvusi didesnė. Vis dėlto, kaip nurodoma atsiliepime, Mokėjimai, kaip momentiniai mokėjimai, buvo įvykdyti nedelsiant, t. y. lėšos į gavėjo sąskaitą buvo pervestos ne vėliau kaip per 10 sek. Tokiu atveju, kaip nustatyta Mokėjimų įstatymo 44 straipsnyje, mokėjimo nurodymo atšaukimas yra galimas tik su lėšų gavėjo sutikimu. Bankas atkreipia dėmesį, kad, pareiškėjai paskambinus į banką pranešti apie sukčiavimo ataką, banko darbuotoja atliko ir kitus tokiose situacijose būtinus atlikti veiksmus, siekdama apsaugoti likusias lėšas pareiškėjos banko sąskaitose: užblokavo pareiškėjos interneto banko paskyrą, dėl „Smart-ID" paskyros atšaukimo rekomendavo kreiptis į „Smart-ID" išleidėjos bendrovės *SK ID Solutions AS* Lietuvos filialą, taip pat rekomendavo dėl sukčiavimo kreiptis į teisėsaugos institucijas, o pats bankas kreipėsi į lėšų gavėjo mokėjimo paslaugų teikėją dėl lėšų grąžinimo.

Pagal Mokėjimų įstatymo 46 straipsnį, mokėjimo paslaugų teikėjas privalo užtikrinti, kad po mokėjimo nurodymo gavimo mokėjimo operacijos suma būtų įskaityta į mokėjimo nurodyme nurodyto gavėjo sąskaitą minėtame straipsnyje nustatytais terminais, o Mokėjimų įstatymo 51 straipsnio 1 dalyje nustatyta mokėjimo paslaugų teikėjo atsakomybė už mokėtojo inicijuotos mokėjimo operacijos neįvykdymą, netinkamą ar pavėluotą įvykdymą. Aplinkybė, kad

pareiškėjos ginčijami Mokėjimai iš tiesų yra neautorizuoti, nors ir atitiko pareiškėjos ir banko sutartą sutikimo atlikti mokėjimo operaciją davimo tvarką, paaiškėjo vėliau, nei šie Mokėjimai buvo patvirtinti ir įvykdyti, ir iki to laiko, kol pareiškėjos interneto banko paskyra buvo užblokuota, taigi, konstatuotina, kad bankas neturėjo teisės aktuose nustatyto pagrindo tokių mokėjimo nurodymų nevykdyti.

4. Dėl banko teikiamų mokėjimo paslaugų saugumo

Pareiškėja, grįsdama bankui keliamą reikalavimą kompensuoti nuostolius, susijusius su Mokėjimo įvykdymu, nurodo ir tai, kad bankas nesiėmė reikiamų veiksmų tam, kad apsaugotų pareiškėjos banko sąskaitoje esančių lėšų saugumą ir Mokėjimų sumos nebūtų pervestos sukčiams.

Kaip minėta, nagrinėdamas ginčus Lietuvos bankas neatlieka patikrinimų tam, kad nustatytų, ar buvo pažeisti finansų įstaigų veiklai keliami teisės aktų reikalavimai. Lietuvos bankas remiasi ginčo šalių pateiktais konkrečiais įrodymais, kurių pagrindu priima sprendimą. Atsižvelgiant į tai, būtina konstatuoti, kad ginčo byloje nėra jokių duomenų, galinčių patvirtinti pareiškėjos nurodytą aplinkybę, kad bankas nesiėmė reikiamų veiksmų, kad apsaugotų pareiškėjos banko sąskaitose esančias lėšas, o įvykdydamas Mokėjimus būtų pažeidęs finansų rinką reglamentuojančių teisės aktų reikalavimus.

Kreipimesi teigdama, kad banko vidaus sistemos yra nesaugios, pareiškėja papildomai nurodo, kad bankas nėra jos informavęs, kaip ir kada buvo nustatyti pareiškėjos sąskaitoms banke taikomi mokėjimo operacijų limitai ir kokiu būdu banko mokėjimo sistemos užtikrina nestandartinių mokėjimų saugumą. Atsižvelgdamas į šį pareiškėjos teiginį, bankas atsiliepime nurodė, kad paaiškinimus dėl mokėjimo operacijų limitų bankas pareiškėjai yra pateikęs atsakyme į pareiškėjos pretenziją. Bankas taip pat pažymėjo, kad Mokėjimo operacijų stebėseną ir stabdymą bankas vykdo taip, kad nenukentėtų banko klientų interesai. Banko teigimu, praktikoje pasitaiko atvejų, kai klientai vykdo mokėjimo operacijas, skaidydami jas dalimis, nes gavėjo mokėjimo paslaugų teikėjai gali būti (būna) nustatę limitą vienos įskaitymo operacijos sumai. Bankas pažymi, kad šiuo konkrečiu atveju pareiškėjos ginčijami Mokėjimai nepasižymėjo nestandartiškumu.

Vien aplinkybė, kad Mokėjimai buvo įvykdyti, kaip pareiškėja nurodo, sukčių naudai, savaime nepagrindžia aplinkybės, kad banko taikytos saugumo priemonės, net ir tuo atveju, jei būtų nustatyta, kad pareiškėja elgėsi itin apdairiai su jai išduotomis mokėjimo priemonėmis ir jų personalizuotais saugumo duomenimis, šiuo konkrečiu atveju buvo ne tik nepakankamos, bet ir neatitinkančios teisės aktų reikalavimų, ir tai galėjo nulemti Mokėjimų įvykdymą, dėl to galėtų kilti ir atitinkama banko civilinė atsakomybė Mokėjimų nulemtus nuostolius pareiškėjai kompensuoti. Kaip minėta, duomenų, kad bankas būtų nevykdęs finansų rinką reglamentuojančių teisės aktų reikalavimų, nenustatyta.

Pati pareiškėja savo deklaratyvių teiginių, kad banko taikytos priemonės ir veiksmai buvo nepakankami tam, kad apsaugotų pareiškėjos banko sąskaitoje esančias lėšas, jokiais duomenimis nepagrindė, pareiškėja taip pat nenurodė, kokių priemonių, jos vertinimu, bankas turėjo imtis, kad jos prašymas grąžinti ginčijamų Mokėjimų lėšas būtų sėkmingai įvykdytas (t. y. Mokėjimų lėšos grąžintos į pareiškėjos banko sąskaitą)-. Priešingai, įvertinus nustatytas aplinkybes, padaryta išvada, kad pareiškėjos nuostolius dėl Mokėjimų įvykdymo, prieš tai tretiesiems asmenims pasisavinus pareiškėjos mokėjimo priemonių personalizuotus saugumo duomenis, šiuo konkrečiu atveju nulėmė būtent pačios pareiškėjos itin neatsargūs veiksmai.

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 Mokėjimų 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