LIETUVOS BANKO
TEISĖS IR LICENCIJAVIMO DEPARTAMENTO
DIREKTORIUS

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

2022 m. lapkričio 23 d. Nr. 429-591
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 1 d. 10 val. 20 min. telefonu gavo SMS pranešimą su nuoroda. Paspaudus trečiųjų asmenų atsiųstą nuorodą, atsidarė netikras banko interneto puslapis, imituojantis banko interneto banko puslapį, kuriame 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 3 332 Eur vertės mokėjimą, kuris buvo patvirtintas pareiškėjos naudojamos atpažinties priemonės „Smart-ID" paskyros PIN2 kodo suvedimu (toliau – Mokėjimas).

2022 m. birželio 1 d. 10:27 val. pareiškėja kreipėsi į banką telefonu, norėdama pranešti apie sukčiavimo atvejį. Telefoninio pokalbio metu banko darbuotoja blokavo pareiškėjos interneto banko paskyrą ir rekomendavo kreiptis į teisėsaugos institucijas.

2022 m. birželio 1 d. bankas kreipėsi į lėšų gavėjo mokėjimo paslaugų teikėją Verse Payments Lithuania UAB dėl Mokėjimo sumos grąžinimo, tačiau lėšų gavėjo mokėjimo paslaugų teikėjas nepateikė atsakymo bankui dėl prašymo grąžinti Mokėjimo lėšas. Apie tai bankas informavo pareiškėją 2022 m. liepos 1 d. pranešimu pareiškėjos interneto banko paskyroje.

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

Kreipimesi pareiškėja pripažįsta atskleidusi, t.y. suklastotoje banko interneto banko svetainėje suvedusi savo mokėjimo priemonių personalizuotus saugumo duomenis, kurie įgalino trečiuosius asmenis jos vardu inicijuoti Mokėjimą. Vis dėlto, pareiškėja mano, kad tokius jos veiksmus lėmė banko spaudimas tą pačią dieną kuo greičiau pateikti prašomus dokumentus, susijusius su pareiškėjai suteikta būsto paskola. Pareiškėjos teigimu, trečiųjų asmenų banko vardu siųsta SMS žinutė jai atrodė susijusi su banko prašymu kuo skubiau pateikti prašomus dokumentus, todėl ji nedvejojusi paspaudė pranešime pateiktą nuorodą.

Pareiškėja taip pat pažymi, kad banko mobiliosios programėlės veikimas dažnai sutrinka, todėl prisijungiant prie jos, pareiškėjos prašoma suvesti ne tik PIN1, bet ir PIN2 kodą, ir ši aplinkybė, pareiškėjos teigimu, galėjo suklaidinti ją dėl PIN2 suvedimo reikšmės bei pasekmių Mokėjimo tvirtinimo metu. Be to, pareiškėjos manymu, bankas per vėlai sureagavo į jos prašymą atšaukti Mokėjimą ir tai apsunkino pareiškėjo galimybes susigrąžinti šios mokėjimo operacijos lėšas. Kreipimesi pareiškėja prašo rekomenduoti bankui kompensuoti pareiškėjai jos ginčijamo Mokėjimo sumą.

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 ko tretieji asmenys galėjo ne tik pareiškėjos vardu inicijuoti Mokėjimą, bet ir ginčijamas Mokėjimas buvo tinkamai patvirtintas.

Atsiliepime pažymima, kad operacijų tvirtinimui bankas taiko papildomą kliento ir jo operacijų autentifikavimą, taip siekiant suteikti galimybę klientui įsitikinti inicijuojamos

operacijos teisėtumu - klientams įvykdžius visas būtinas sąlygas, sutartas tarp banko ir kliento, kuriomis yra tinkamai identifikuojama kliento inicijuota operacija, bankas įsipareigoja tokias operacijas įvykdyti. Bankas nurodo, kad Mokėjimo 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, tokiu būdu suteikdama galimybę sukčiams inicijuoti ir atlikti Mokėjimą. Banko teigimu, jis deda 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 Mokėjimo įvykdymo.

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 mano, kad banko veiksmai – raginimas kuo skubiau atsiųsti prašomus dokumentus Mokėjimo įvykdymo dieną, dažnai nesklandus banko mobiliosios programėlės veikimas, dėl ko prisijungti prie banko mobiliosios programėlės papildomai prašoma suvesti atpažinties priemonės „Smart-ID" PIN2 kodą, prisidėjo prie to ar net lėmė tai, kad šiuo atveju pareiškėja suvedė „Smart-ID" PIN2 kodą, kuriuo patvirtintas trečiųjų asmenų inicijuotas Mokėjimas. Be to, pareiškėjos vertinimu, bankas nesiėmė reikiamų veiksmų tam, kad padėtų pareiškėjai atgauti jos ginčijamo Mokėjimo sumas, todėl bankas turėtų kompensuoti pareiškėjai su Mokėjimo įvykdymu susijusius jos nuostolius (Mokėjimo sumą). 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 savo naudojamos „Smart-ID" paskyros PIN2 kodo suvedimu, 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; 3) bankas tinkamai reagavo į pareiškėjos pranešima apie neteisėtą jos mokėjimo priemonės panaudojimą ir pagrįstai įvykdė ginčijamą Mokėjimą.*

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 duomenis, kurie patvirtina šalių (taigi, tiek pareiškėjos, tiek ir banko) neginčijamą aplinkybę, 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 (šiuo atveju – pareiškėjos) tapatybės nustatymo procesą, bankas mano, kad nėra pagrindo laikyti Mokėjimo neautorizuotu.

Kaip matyti iš banko paaiškinimų, darydamas išvadą, kad Mokėjimas buvo tinkamai pareiškėjos patvirtintas ir laikytinas autorizuotu, bankas papildomai nevertino Mokėjimo inicijavimo ir patvirtinimo aplinkybių, kuriuo metu, aplinkybėmis ir (arba) 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. Tad nors bankas kartu su atsiliepimu pateikė jo vidaus sistemose užfiksuotus duomenis, pagrindžiančius, kad prieš Mokėjimo įvykdymą, siekiant prisijungti prie pareiškėjos interneto banko paskyros, buvo panaudoti interneto banko prisijungimo duomenys ir suvestas „Smart-ID" PIN1 kodas, o pats 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, tačiau vien šie duomenys, Lietuvos banko vertinimu, savaime dar neįrodo, kad Mokėjimas iš tiesų atliktas pareiškėjos sutikimu (pareiškėjos valia).

Vadinasi, bankas, siekdamas pagrįsti teiginį, kad Mokėjimams 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). Tačiau ginčo nagrinėjimo metu nustatyta, kad pareiškėja, priešingai, nei nurodyta aptariamose nuostatose, šiuo atveju 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 tariamam paskyros atblokavimui.

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 tokiai mokėjimo operacijai, 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 kaip jie atitinka su banku sutartos sutikimo mokėjimo operacijai atlikti 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. Vis dėlto, Lietuvos bankas pažymi, kad valia yra esminis kiekvienos sandorio, kaip teisinio veiksmo, kuriuo siekiama suskurti 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 mokėjimo operacijai 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 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 atvaizduojama 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 *sebvaldymovaldymo.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 apribojimo panaikinimui, o ne inicijuoti mokėjimo nurodymus lėšų pervedimams iš banke esančios pareiškėjos sąskaitos – vadinasi, pareiškėja valios inicijuoti Mokėjimo, kaip ir jo autorizuoti, neturėjo.

Ginčo byloje esantys įrodymai, tarp jų ir pirmiau aptarti įrodymai dėl Mokėjimo inicijavimo ir įvykdymo aplinkybių, kurių nepaneigė banko paaiškinimai ir pateikti vidinės sistemos duomenys apie tai, kad Mokėjimui 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. Tai galėjo suklaidinti pareiškėją dėl toliau atliekamų veiksmų esmės ir pobūdžio. Vadinasi, duomenų, kad ginčo šalių susitarime aptarti sutikimo mokėjimo operacijai formalūs išoriniai

[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).

veiksmai atitiko pareiškėjos valią, kitaip tariant, kad pareiškėja, žinojo, suprato ir pati išreiškė savo valią autorizuoti Mokėjimą šalių sutarta tvarka, ginčo byloje nėra.

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. T.y. 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 Mokėjimui šalių sutarta forma ir tvarka, nepatvirtina ginčo nagrinėjimo metu nustatytos aplinkybės. Todėl, 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 apribojimų panaikinimui, galima daryti išvadą, kad Mokėjimo inicijavimas ir patvirtinimas neatitiko pačios pareiškėjos valios, nors formaliai (išoriniais požymiais) 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 šio ginčo nagrinėjimo metu 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 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 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. T.y. 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 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 1 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 ant pranešime pateiktos nuorodos 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 pareiškėjai žinomus: „Smart-ID" paskyros PIN1 kodą - po šio kodo suvedimo tretieji asmenys prisijungė prie pareiškėjos interneto banko paskyros, ir „Smart-ID" paskyros PIN2 kodą – suvesdama šį kodą pareiškėja patvirtino trečiųjų asmenų, pareiškėjos vardu, suformuotą Mokėjimą.

Pirmiau konstatuotas aplinkybes patvirtina ir pačios pareiškėjos kreipimesi pateikti paaiškinimai. Pareiškėja nurodo ginčijamo Mokėjimo įvykdymo dieną bendravusi su banko darbuotojais dėl banko nurodytų dokumentų, susijusių su pareiškėjai suteikta būsto paskola, pateikimo bankui. Pareiškėjos teigimu, „<...>10:24 jausdama aiškų spaudimą iš banko (žinutės kas 5 minutės ir grasinimas, kad paskyra apribota), pabaigiau išsiųsti trūkstamus duomenis bankui ir paspaudžiau nuorodą, norėdama suprasti, kodėl šis trūkstamas dokumento patikslinimas iššaukė poreikį net riboti mano paskyrą. Paspaudus nuorodą, buvau nukreipta į SEB interneto banko prisijungimą (netikrą, bet tuo metu jausdama banko spaudimą to nepastebėjau), kur buvau paprašyta suvesti savo banko ID ir SMART ID PIN1 (kaip tradiciškai jungiantis prie interneto banko), tada po kurio laiko buvau paprašyta suvesti SMART ID PIN2. Suvesti SMART ID PIN2 yra tekę pasirašant dokumentus (ne tik darant pavedimą), tad įvertinusi grasinimą kaip svarbų veiksmą, suvedžiau ir SMART ID PIN 2. Kai suvedžiau SMART ID PIN2, buvo iškarto nurašyta 3332 Eur nuo mano sąskaitos <...>."

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 tapatybės patvirtinimui, 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), 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: pagal banko pateiktus jo informacinių sistemų žurnalo duomenis, pareiškėjai jos naudojamoje „Smart-ID" paskyroje suvedant PIN2 kodą Mokėjimo tvirtinimo metu buvo rodomas tekstas „3 332,00 EUR i saskaita ***4862. Patvir". Bankas pateikė duomenis, kad Mokėjimas buvo patvirtintas būtent pareiškėjos naudojamos atpažinties priemonės - „Smart-ID" paskyros, PIN2 kodo suvedimu.

Taigi, remiantis ginčo byloje esančiais įrodymais, pareiškėjai, prieš suvedant savo

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

naudojamos „Smart-ID" paskyros PIN 2 kodą, atitinkamame „Smart-ID" programėlės pranešime buvo nurodyta, kokiu tikslu pareiškėjos tai prašoma padaryti.

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.

Visų pirma, kaip jau buvo konstatuota pirmiau, pareiškėjos ginčijamas Mokėjimas buvo patvirtintas pačios pareiškėjos naudojamos „Smart-ID" paskyros PIN2 kodo suvedimu. 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 Mokėjimo tvirtinimo metu, pakankamai aiškiai ir nedviprasmiškai informavo pareiškėją, kokiu tikslu jos tai padaryti prašoma – t.y. kad PIN2 kodo suvedimu 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.

Nors pareiškėja pripažįsta suklastotoje banko interneto banko svetainėje suvedusi konfidencialią informaciją, t.y. savo interneto banko atpažinimo kodą ir savo asmens kodą, taip pat suvedusi jos naudojamos „Smart-ID" programėlės PIN kodus, atlikusi, kaip pati teigia, „skubotą žingsnį", tačiau mano, kad tą lėmė iš banko patirtas spaudimas. Toks pareiškėjos teiginys vertintinas kritiškai: pagal ginčo bylos duomenis, Mokėjimo įvykdymo dieną pareiškėja bendravo su banko darbuotojais dėl banko prašomų dokumentų pateikimo, ir gavo banko išsiųstą SMS žinutę bei el. laišką, raginančius pareiškėją pateikti trūkstamus duomenis. Vis dėlto, vertinti tokius banko veiksmus kaip neatitinkančius normalios bendravimo su klientais praktikos ir darančius spaudimą, juo labiau, kaip skatinančius imtis neapdairių veiksmų, pavyzdžiui, suvesti atpažinties priemonės PIN kodus, neskaitant tai padaryti prašančių pranešimų turinio, nėra pagrindo.

Sprendžiant dėl pareiškėjos neatsargumo laipsnio, taip pat būtina atkreipti dėmesį į tai, kad trečiųjų asmenų pareiškėjui siųsta SMS žinutė informavo pareiškėją apie tai, 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: ji buvo siųsta banko vardu, nuorodos pavadinime naudojamas banko pavadinimas. Kita vertus, pastebėtina ir tai, kad SMS žinutėje pateikta nuoroda į tariamą banko interneto banko svetainę – *sebvaldymasvaldymas.com*, visiškai neatitinka tikrosios banko interneto banko svetainės adreso[4] ir neturi jokių sąsajų su interneto banke teikiamomis paslaugomis ar raginimu imtis veiksmų paskyros apribojimo panaikinimui.

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 kas pagrįstų protingai apdairų pareiškėjos siekį veikti žinutės nurodymais. Kaip pagrindžia banko kartu su atsiliepimu pateikti duomenys, pareiškėjai ginčijamo Mokėjimo metu suvedant PIN2 kodą, jai 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 apribojimų panaikinimui.

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 – 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.

Banko atsakomybę dėl įvykdyto neautorizuoto Mokėjimo, kartu ir tai, kad pareiškėjos elgesys šiuo atveju nevertintinas kaip labai neatsargus, pareiškėja grindžia ir aplinkybe, kad, jos teigimu, banko mobilioji programėlė dažnai netinkamai veikia, įdiegus šios programėlės atnaujinimus, prisijungimą prie programėlės reikia užbaigti suvedant „Smart-ID" paskyros PIN2 kodą, kuris įprastai naudojamas mokėjimams autorizuoti, dokumentams pasirašyti ir kitiems veiksmams tvirtinti. Tokie naudojimosi banko mobiliąja programėle ypatumai, pareiškėjos vertinimu, klaidina ją, kaip vartotoją, ir taip pat lėmė tai, kad pareiškėja nedvejodama suvedė savo „Smart-ID" paskyros PIN2 kodą, taip patvirtindama Mokėjimą, kurio ji neinicijavo ir įvykdyti nesiekė.

Vis dėlto, šie pareiškėjos teiginiai vertintini kaip nepagrįsti: pateikdamas papildomus paaiškinimus dėl pareiškėjos kreipimesi išdėstytų teiginių, bankas paaiškino, kad siekiant prisijungti prie banko mobiliosios programėlės, turi būti suvestas tik „Smart-ID" PIN1 kodas, o PIN2 kodas yra suvedamas siekiant patvirtinti atliekamus veiksmus. Šiuo atveju, kaip pažymėjo bankas, trečiųjų asmenų inicijuotas Mokėjimas buvo patvirtintas pareiškėjai suvedus jos naudojamos „Smart-ID" paskyros PIN2 kodą, pačiai pareiškėjai nesinaudojus banko mobiliąja programėle. Kaip nustatyta, nagrinėjamu atveju prie suklastotos banko interneto banko svetainės pareiškėja jungėsi paspausdama SMS žinutėje pateiktą nuorodą (vadinasi, ne naudodamasi banko mobiliąja programėle), atliekamus veiksmus – t.y. prisijungimą prie sąskaitos, kaip pati pripažįsta, tvirtindama „Smart-ID" paskyros PIN2 kodu. Todėl, net ir nevertinant pareiškėjos teiginio pagrįstumo – t.y. ar naudojimosi banko mobiliąja programėle ypatumai yra aiškūs, suprantami ir neklaidinantys banko klientų, ar pati banko mobilioji programėlė veikia tinkamai, manytina, kad aptartos aplinkybės pagrindžia pačios pareiškėjos būtino atidumo nebuvimą vertinamomis aplinkybėmis. T.y. pareiškėja ne tik paspaudė nuorodą į suklastotą banko interneto banko svetainę, atskleisdama ten savo mokėjimo priemonių personalizuotus saugumo duomenis, bet ir neperkaičiusi 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 pagal banko pateiktus duomenis, banko interneto banko paslaugomis su mobiliajame telefone susikurta „Smart-ID" paskyra, pareiškėja naudojasi dar nuo 2017 m. spalio 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.

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.

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

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 negincijamos neautorizuotos mokėjimo operacijos įvykdymo aplinkybės. Vis dėlto, šiuo atveju ginčo nagrinėjimo metu 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. Tai, kad šiuo atveju atliko skubotus veiksmus, kreipimesi pripažino ir pati pareiškėja. Tokiu būdu 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, kuriam patvirtinti duotas pačiai pareiškėjai savo „Smart-ID" paskyroje suvedus paskyros PIN2 kodą, prieš tai neperskaičius ir (ar) neįvertinus „Smart-ID" programėlės pranešimo 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, ji iškart paskambino į banką, siekdama pranešti apie sukčiavimo atvejį ir užblokuoti savo sąskaitą, tačiau bankas į lėšų gavėjo mokėjimo paslaugų teikėją dėl mokėjimo nurodymo įvykdyti Mokėjimą atšaukimo kreipėsi tik praėjus 3 valandoms nuo pareiškėjos skambučio. Pareiškėja mano, kad jei bankas būtų greičiau reagavęs ir anksčiau kreipęsis į gavėjo mokėjimo paslaugų teikėją, Mokėjimo sumos 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, pareiškėjos ginčijamas Mokėjimas buvo įvykdytas ir iš pareiškėjos sąskaitos nurašytas 2022 m. birželio 1 d. 10:24 val. – taigi, dar iki pareiškėjos pirmojo skambučio bankui, kuris banko informacinių sistemų duomenimis įvyko 10:27 val., ir atitinkamai iki pareiškėjos pranešimo apie mokėjimo priemonės paradimą bei neautorizuotą jos panaudojimą. Tai reiškia, kad pareiškėja į banką dėl ginčijamo Mokėjimo paskambino jau po to, kai sutikimas minėtai mokėjimo operacijai buvo duotas ir pati neautorizuota bei pareiškėjos ginčijama mokėjimo operacija (t.y. Mokėjimas) jau buvo įvykdyta.

---

[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 .

Lietuvos bankas neturi pakankamai duomenų, kurie patvirtintų ar paneigtų pareiškėjos teiginį, kad jei bankas būtų iškart (t.y. anksčiau nei per tris valandas nuo pranešimo apie ginčijamą Mokėjimą) kreipęsis į lėšų gavėjo mokėjimo paslaugų teikėją dėl Mokėjimo lėšų grąžinimo pareiškėjai, tikimybė šias lėšas atgauti būtų buvusi didesnė. Vis dėlto, kaip nurodoma atsiliepime, Mokėjimai, kaip momentiniai mokėjimai, buvo įvykdyti nedelsiant - lėšos į gavėjo sąskaitą buvo pervestos ne vėliau kaip per 10 sek. Tokiu atveju, kaip nustato Mokėjimų įstatymo 44 straipsnio nuostatos, mokėjimo nurodymo atšaukimas yra galimas tik lėšų gavėjo sutikimu. Bankas atsiliepime papildomai pažymėjo, kad lėšų gavėjo mokėjimo paslaugų teikėjai (šiuo atveju Verse Payments Lithuania UAB) neturi prievolės teikti atsakymo bankui dėl pateikto prašymo grąžinti lėšas, nes privalomas bendradarbiavimas tarp mokėjimo paslaugų teikėjų nėra teisės aktų reglamentuotas ir įprastai vyksta geranoriškumo principu.

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 ginčijamas Mokėjimas iš tiesų yra neautorizuotas, nors ir atitiko pareiškėjos ir banko sutartą sutikimo mokėjimo operacijai davimo tvarką, paaiškėjo vėliau, nei šis Mokėjimas buvo patvirtintas ir įvykdytas ir iki to laiko, kol pareiškėjos interneto banko paskyra buvo blokuota. Tai reiškia, kad šiuo atveju bankas neturėjo teisės aktuose nustatyto pagrindo tokio mokėjimo nurodymo nevykdyti.

Todėl, įvertinus visa tai, kas išdėstyta pirmiau, ir nustačius, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, darytina išvada, kad pareiškėjos banko atžvilgiu 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