



**LIETUVOS BANKO
TEISĖS IR LICENCIJAVIMO DEPARTAMENTO
DIREKTORIUS**

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

2025-09-08 Nr. 429-203
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:

2025 m. gegužės 19 d. iš pareiškėjos banko sąskaitos panaudojant tik pareiškėjai žinomus personalizuotus saugos duomenis lėšų gavėjui *duomenys neskelbiami* (toliau – lėšų gavėjas) buvo atlikta 1 500 Eur mokėjimo operacija (toliau – ginčijama mokėjimo operacija).

Ginčo byloje nustatyta, kad pareiškėja, turėdama tikslą prisijungti prie VĮ Registrų centras Google paieškos sistemoje suvedė VĮ Registrų centras raktinius žodžius, pateko į minėtos įstaigos puslapį ir jungdamasi per elektroninės valdžios vartų platformą, paspaudė banko logotipą. Paspaudusi aktyvią nuorodą, pareiškėja buvo nukreipta į suklastotą banko interneto banko puslapį, kuriame buvo prašoma įvesti tik pareiškėjai žinomus personalizuotus saugos duomenis, reikalingus prisijungti prie interneto banko: interneto banko atpažinimo ir asmens kodą bei prisijungimą patvirtinti pareiškėjos naudojamos atpažinimo priemonės „Smart-ID“ paskyros PIN1 kodu. Pareiškėjai suvedus šiuos duomenis, tretieji asmenys įgijo galimybę prisijungti prie pareiškėjos banko sąskaitos ir inicijuoti ginčijamą mokėjimo operaciją. Ginčijamą mokėjimo operaciją pareiškėja patvirtino savo mobiliajame telefone suveddama tik jai vienai žinomą „Smart-ID“ PIN2 kodą.

Remdamasis visa surinkta informacija, bankas priėmė sprendimą atsisakyti pareiškėjai atlyginti jos patirtus nuostolius, nes nustatė, kad ginčijama mokėjimo operacija buvo įvykdyta dėl pareiškėjos itin neatsargių veiksmų. Banko nuomone, tai ir lėmė, kad pareiškėja patyrė nuostolių. Pareiškėja su tuo nesutiko, todėl tarp šalių kilo ginčas.

Kreipimesi į Lietuvos banką pareiškėja prašo įpareigoti banką grąžinti ginčijamos mokėjimo operacijos metu iš jos banko sąskaitos nurašytas lėšas, t. y. grąžinti 1 500 Eur. Pareiškėja Lietuvos bankui paaiškino, kad „2025 m. gegužės 18 d. apie 17 val. jungiantis prie Elektroninės valdžios vartų platformos, buvo neteisėtai pasinaudota mano Smart-ID programa – paprašyta patvirtinti PIN1 ir PIN2 kodus, prisijungiant prie SEB banko (toliau – Bankas), ir iš man priklausančios SEB banko sąskaitos Nr. *duomenys neskelbiami* buvo neteisėtai nurašyta 1 500 eurų (vienas tūkstantis penki šimtai eurų). <...>. Pinigų nurašymas įvyko 2025 m. gegužės 19 d.“ Pareiškėja teigė, kad ji, jungdamasi prie Elektroninės valdžios vartų platformos, neturėjo tikslo atlikti jokių finansinių operacijų, o „Smart-ID paprašius patvirtinti PIN kodą, buvo pateikta informacija apie sutarties pasirašymą su SEB banku, o ne apie piniginę operaciją. Todėl toks prisijungimas nesukėlė įtarimų“. Pareiškėja teigė, kad prieš suvedant „Smart-ID“ PIN2 kodą bankas jai nerodė informacijos apie tvirtinamą mokėjimo operaciją – lėšų gavėją ir sumą.

Pareiškėja taip pat paaiškino, kad pakartotinai paprašius įvesti „Smart-ID“ PIN2 kodą pareiškėja nedelsdama sureagavo ir kelis kartus el. paštu kreipėsi į banką bei skambino bankui trumpuoju banko numeriu, tačiau jai nepavyko susisiekti su banku.

Pareiškėja teigė, kad ji nuostolių patyrė dėl to, kad bankas neužtikrino lėšų esančių jos banko sąskaitoje saugumo, tinkamai nevykdė mokėjimo operacijų stebėsenos, neįdiegė jokios rizikų valdymo sistemos, o pareiškėjai pranešus apie neautorizuotos mokėjimo operacijos iš jos banko sąskaitos įvykdymą, bankas tinkamai neveikė, kad ginčijamos mokėjimo operacijos lėšos būtų sugrąžintos.

Atsiliepime į pareiškėjos kreipimąsi bankas nurodo nesutinkąs su pareiškėjos reikalavimu ir prašo jį atmesti. Banko teigimu, pareiškėjos veiksmai su savo mokėjimo priemone gali būti vertinami kaip labai neatsargūs, nes ji į sukčių suklastotą Elektroninės valdžios vartų platformą suvedė savo personalizuotus saugos duomenis, reikalingus prisijungti prie interneto banko paskyros (banko atpažinimo, asmens ir „Smart-ID“ PIN1 kodus). Be to, pareiškėja ginčijamą mokėjimo operaciją pati patvirtino, suveddama „Smart-ID“ PIN2 kodą, o bankas prieš pareiškėjai suvedant „Smart-ID“ PIN2 kodą mobiliojo telefono „Smart-ID“ lange rodė tiek ginčijamos mokėjimo operacijų sumą, tiek ir lėšų gavėjo sąskaitos numerį. Bankas teigia, kad pareiškėja neginčija fakto, jog ji pati suvedė visus savo personalizuotus saugos duomenis, įskaitant ir „Smart-ID“ PIN2 kodą. Banko vertinimu, tai, kad pareiškėja, veddama savo personalizuotus saugos duomenis, įskaitant ir „Smart-ID“ PIN2 kodą, nors jai aiškiai buvo rodoma šio kodo vedimo paskirtis, kritiškai nevertino savo atliekamų veiksmų, rodo, jog ji dėl didelio neatsargumo neišsaugojo savo personalizuotų saugos duomenų, dėl to tretieji asmenys jais galėjo pasinaudoti ir be pareiškėjos žinios inicijuoti ginčijamą mokėjimo operaciją.

Bankas pažymėjo, kad iki ginčijamų mokėjimo operacijų įvykdymo bankas pareiškėją buvo informavęs apie sukčiavimo grėsmes naudojantis mokėjimo paslaugomis¹. Pareiškėjai siųstais pranešimais bankas ją informavo apie saugų naudojimąsi banko nuotoliniais kanalais. Taip pat bankas pažymėjo, kad jis savo interneto svetainėje skelbia informaciją apie dažniausiai pasitaikančias sukčiavimo atakas ir teikia patarimus banko klientams, kaip išvengti sukčių pinklių.

Taip pat bankas paaiškino, kad gavęs pareiškėjos pretenziją dėl neautorizuotos mokėjimo operacijos įvykdymo, tą pačią dieną kreipėsi į lėšų gavėją, tačiau lėšų sugrąžinti nepavyko.

Atsižvelgdamas į visas pirmiau nurodytas aplinkybes, bankas prašė atmesti pareiškėjos reikalavimą kaip nepagrįstą.

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

Vadovaujantis Lietuvos banko valdybos 2012 m. sausio 26 d. nutarimu Nr. 03-23 patvirtintų Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių 44 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 vartojimo ginčą, Lietuvos bankas neatlieka Lietuvos Respublikos Lietuvos banko įstatymo 42¹ straipsnyje reglamentuotų patikrinimų faktinėms aplinkybėms dėl Lietuvos banko kompetencijai priskirtų teisės aktų reikalavimų laikymosi ir (arba) vartotojo įtariamo galimo šių reikalavimų pažeidimo nustatyti ir įvertinti. Nagrinėdamas ginčą, Lietuvos bankas atlieka ginčo šalių pateiktų įrodymų vertinimą ir jo pagrindu priima sprendimą.

Pareiškėjos ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjai ginčijamos mokėjimo operacijos metu iš jos sąskaitos banke pervestą sumą. Pareiškėja neigia autorizavusi ginčijamą mokėjimo operaciją ir teigia, kad bankas neužtikrino lėšų jos banko sąskaitoje saugumo, dėl to ji patyrė nuostolių, kuriuos prašo atlyginti. Banko teigimu, pareiškėjos veiksams būdingas didelis neatsargumas, todėl bankas negali būti įpareigotas jai grąžinti ginčijamos mokėjimo operacijos sumos.

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.

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).

Pareiškėjos nurodytos aplinkybės, kad ginčijama mokėjimo operacija nėra jos autorizuota, o pareiškėjos personalizuotus saugumo duomenis tretieji asmenys gavo apgaulės būdu, bankas atsiliepime neginčija. Priešingai, bankas savo paaiškinimuose nurodo, kad dėl pareiškėjos

¹ 2024 m. gegužės 17 d., 2024 m. rugpjūčio 14 d., 2024 m. spalio 8 d., 2024 m. lapkričio 19 d., 2025 m. vasario 14 d. siuntė pranešimus į pareiškėjos elektroninį paštą.

atskleistų duomenų tretieji asmenys įgijo galimybę inicijuoti ginčijamą mokėjimo operaciją. Dėl šios priežasties yra akivaizdu, kad ginčijamos mokėjimo operacijos inicijavimas ir patvirtinimas neatitiko pačios pareiškėjos valios, nors formaliai (pagal išorinius požymius) ir sutapo su pareiškėjos ir banko sutarta sutikimo atlikti mokėjimo operaciją davimo forma ir tvarka. Atsižvelgdamas į tai, Lietuvos bankas daro išvadą, kad ginčijama mokėjimo operacija, atlikta nesant pareiškėjos valios ir neišreiškus valinių veiksmų patvirtinti ginčijamą mokėjimo operaciją, laikytina neautorizuota.

Siekdamas išspręsti tarp šalių kilusį ginčą ir įvertinti pareiškėjos bankui keliamo reikalavimo pagrįstumą, Lietuvos bankas vertins: 1) ar bankas, atsisakydamas grąžinti pareiškėjai ginčijamos mokėjimo operacijos metu pervestas lėšas, pagrįstai rėmėsi Mokėjimų įstatymo 39 straipsnio 3 dalimi; 2) ar bankas užtikrino lėšų pareiškėjos banko sąskaitoje saugumą.

1. Dėl banko atsisakymo grąžinti pareiškėjai ginčijamos mokėjimo operacijos metu pervestas lėšas.

Mokėjimų įstatymo 39 straipsnio 3 dalyje nustatyta, kad mokėtojai 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.

Taip pat svarbu pažymėti, kad Lietuvos Aukščiausiasis Teismas yra konstatavęs, jog įstatyme nustatyta tokia mokėtojo paslaugų teikėjo atsakomybės už neautorizuotą mokėjimą sistema, pagal kurią mokėtojas turi teisę į neautorizuotos operacijos sumos sugrąžinimą, o mokėtojo paslaugos teikėjas turi pareigą ją sugrąžinti, išskyrus atvejus, jei nustatoma, kad: 1) mokėtojas veikia nesąžiningai; 2) mokėtojas tyčia ar dėl didelio neatsargumo pažeidžia vieną ar kelias Mokėjimų įstatymo 34 straipsnyje nustatytas mokėtojo pareigas, susijusias su mokėjimo priemonėmis ir personalizuotais saugumo duomenimis. Nurodyta mokėtojo paslaugų teikėjo atsakomybės už neautorizuotą mokėjimą sistema reiškia griežtąją mokėtojo paslaugų teikėjo atsakomybę už atliktas neautorizuotas mokėjimo operacijas, t. y. atsakomybę be kaltės. Kita vertus, mokėtojo paslaugų teikėjo atsakomybė be kaltės neeliminuoja paties mokėtojo pareigos elgtis rūpestingai ir atsakingai. Todėl tuo atveju, jei mokėtojas elgiasi nesąžiningai arba tyčia ar dėl didelio neatsargumo pažeidžia įstatyme jam nustatytas pareigas, paslaugos teikėjas yra atleidžiamas nuo atsakomybės. Ne bet kokių mokėtojo pareigų nevykdymas yra pagrindas atleisti mokėtojo paslaugos teikėją nuo atsakomybės, o būtent Mokėjimų įstatymo 34 straipsnyje nustatytų mokėtojo pareigų, kurios susijusios su mokėjimo priemonėmis ir personalizuotais saugumo duomenimis, be to, paprastas mokėtojo neatsargumas nėra laikomas mokėtojo paslaugos teikėjo atleidimo nuo atsakomybės sąlyga².

Duomenų, kad nagrinėjamu atveju pareiškėja galėjo veikti nesąžiningai arba tyčia, nėra, todėl galimas mokėtojo sukčiavimas, kaip pagrindas atleisti mokėtojo mokėjimo paslaugų teikėją nuo pareigos atlyginti mokėtojai nuostolius dėl neautorizuotos mokėjimo operacijos įvykdymo, šiame sprendime atskirai nebus plačiau analizuojamas.

Taigi, sprendžiant, ar banko atsisakymas grąžinti pareiškėjai ginčijamos mokėjimo operacijos sumą laikytinas pagrįstu, būtina įvertinti, ar pareiškėjos elgesys, atskleidžiant tretiesiems asmenims personalizuotus saugumo duomenis, vertintinas kaip didelis neatsargumas, dėl kurio su mokėjimo operacijos įvykdymu atsiradę nuostoliai, kaip nustatyta Mokėjimų įstatymo 39 straipsnio 3 dalyje, tektų pačiai pareiškėjai.

Lietuvos Aukščiausiasis Teismas yra išaiškinęs, kad didelis neatsargumas pasireiškia neprotingu arba išskirtiniu rūpestingumo nebuvimu, kai asmuo nėra tiek rūpestingas, kiek akivaizdžiai būtina esamomis aplinkybėmis³. Didelis mokėtojo neatsargumas gali būti konstatuojamas tik tuomet, jei mokėtojas elgėsi labai nerūpestingai. Kad mokėtojas elgėsi labai nerūpestingai, turi įrodyti mokėjimo paslaugų teikėjas, pateikdamas konkrečius tokį elgesį pagrindžiančius įrodymus. Ši įrodinėjimo našta negali būti perkelta mokėtojui⁴.

Dėl mokėtojo neatsargumo laipsnio vertinimo, pagrindinių jo kriterijų ir glaudaus ryšio su ginčo byloje nustatytų individualių specifinių aplinkybių visuma Lietuvos bankas yra ne kartą plačiau pasisakęs savo ginčų nagrinėjimo praktikoje⁵, todėl šiame sprendime bus pasisakoma

² Lietuvos Aukščiausiojo Teismo 2023 m. rugsėjo 12 d. nutartis civilinėje byloje Nr. e3K-3-182-1075/2023, 44 punktas.

³ Lietuvos Aukščiausiojo Teismo 2017 m. balandžio 13 d. nutartis civilinėje byloje Nr. e3K-3-180-378/2017.

⁴ Lietuvos Aukščiausiojo Teismo 2023 m. rugsėjo 12 d. nutartis civilinėje byloje Nr. e3K-3-182-1075/2023, 82 punktas.

⁵ Pavyzdžiui, ginčo byla Nr. 2022-02496.

tik šiai konkrečiai ginčo bylai aktualiais aspektais.

Neautorizuotos mokėjimo operacijos įvykdymo atveju didelis neatsargumas yra sietinas su vienos ar kelių Mokėjimų įstatymo 34 straipsnyje mokėtojai nustatytų pareigų, susijusių su mokėjimo priemone ir personalizuotais saugumo duomenimis, nevykdymu. Kaip yra konstatavęs Lietuvos Aukščiausiasis Teismas, neautorizuotos mokėjimo operacijos atveju mokėjimo paslaugų teikėjas turi įrodyti ne tik tai, kad mokėtojas pažeidė vieną ar kelias Mokėjimų įstatymo 34 straipsnyje nustatytas mokėtojo pareigas, susijusias su mokėjimo priemonėmis ir personalizuotais saugumo duomenimis, bet ir tai, kad tai padarė dėl didelio neatsargumo⁶.

Mokėjimų įstatymo 34 straipsnis nustato mokėtojo pareigą naudotis jam išduota mokėjimo priemone (nagrinėjamu atveju – mokėjimo kortele) pagal jos išdavimą ir naudojimą reglamentuojančias sąlygas, o sužinojus apie jos praradimą, vagystę arba neteisėtą pasisavinimą ar neautorizuotą jos naudojimą, nedelsiant apie tai pranešti mokėjimo paslaugų teikėjui arba jo nurodytam subjektui (Mokėjimų įstatymo 34 straipsnio 1 dalis), taip pat pareigą, gavus mokėjimo priemonę, imtis veiksmų, kad būtų apsaugoti personalizuoti saugumo duomenys (Mokėjimų įstatymo 34 straipsnio 2 dalis).

Bankas mano, kad nuostolius dėl ginčijamos mokėjimo operacijos pareiškėja patyrė dėl savo didelio neatsargumo, t. y. pareiškėja, perduodama tretiesiems asmenims savo prisijungimo prie interneto banko duomenis (banko atpažinimo ir asmens kodus), prisijungimą prie interneto banko patvirtindama „Smart-ID“ programėlės PIN1 kodu, suteikė leidimą tretiesiems asmenims iš jos banko sąskaitos inicijuoti ginčijamą mokėjimo operaciją, kurią pareiškėja pati patvirtino suvedama „Smart-ID“ programėlės PIN2 kodą.

Banko sprendimas nekompensuoti pareiškėjos nuostolių dėl neautorizuotos ginčijamos mokėjimo operacijos įvykdymo galėtų būti vertinamas kaip pagrįstas tik tada, jeigu būtų įrodyta, kad pareiškėja, atskleisdama tam tikrus personalizuotus savo mokėjimo priemonių saugumo duomenis, leido inicijuoti ir net patvirtino ginčijamą mokėjimo operaciją, t. y. elgėsi itin aplaidžiai – buvo labai neatsargi.

Lietuvos bankas, siekdamas nustatyti, ar pareiškėjos elgesys šiuo atveju gali būti laikomas labai neatsargiu, vertino jos elgesį jungiantis prie Elektroninės valdžios vartų platformos, suvedant savo mokėjimo priemonės personalizuotus saugumo duomenis suklustotame interneto banko puslapyje bei patvirtinant atliekamus veiksmus naudojama atpažinties priemone – suvedant „Smart-ID“ programėlės PIN1 ir PIN2 kodus, taip pat banko veiksmus, kurių jis prevenciškai ėmėsi ir imasi tam, kad supažindintų pareiškėją su sukčiavimo elektroninėje erdvėje rizikomis bei tapatybės patvirtinimo priemonės saugaus naudojimo, jos personalizuotų saugumo žymenų suvedimo ir atskleidimo reikšme bei teisinėmis pasekmėmis.

Vertinant pačios pareiškėjos elgesį, svarbu nustatyti, kaip pareiškėja, kaip mokėjimo paslaugų vartotoja, buvo įtikinta atskleisti savo mokėjimo priemonės personalizuotus saugos duomenis, įgalinusius trečiuosius asmenis inicijuoti ginčijamą mokėjimo operaciją.

Lietuvos bankas, įvertinęs pareiškėjos kreipimesi ir banko atsiliepime nurodytas aplinkybes bei kartu su kreipimusi ir atsiliepimu pateiktus duomenis, nustatė, kad prieš ginčijamos mokėjimo operacijos įvykdymą pareiškėja savo iniciatyva jungėsi prie Elektroninės valdžios vartų sistemos, prie kurios prisijungusi paspaudė banko logotipą, pateko į suklustotą banko interneto banko puslapį ir suklustotame banko interneto banko puslapyje suvedė prašomus nurodyti duomenis: banko atpažinimo ir asmens kodus, kurie, kaip paaiškėjo vėliau, buvo nusavinti trečiųjų asmenų (sukčių) ir panaudoti tam, kad būtų prisijungta prie pareiškėjos interneto banko paskyros ir inicijuota ginčijama mokėjimo operacija. Trečiųjų asmenų prisijungimas prie pareiškėjos interneto banko paskyros buvo patvirtintas pačiai pareiškėjai suvedus „Smart-ID“ programėlės PIN1 kodą bei vėliau ginčijamą mokėjimo operaciją pačiai pareiškėjai patvirtintus suvedant „Smart-ID“ programėlės PIN2 kodą.

Kaip pirmiau 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. To paties straipsnio 2 dalyje nurodyta, kad mokėjimo paslaugų vartotojas, gavęs mokėjimo priemonę, privalo imtis veiksmų, kad būtų apsaugoti personalizuoti saugumo duomenys.

Banko ir pareiškėjos santykius reglamentuojančių banko Bendrųjų taisyklių (toliau – Taisyklės) 1 priedo 10 skyriuje nustatyta, kad banko suteiktą mokėjimo priemonę ir su ja

⁶ Lietuvos Aukščiausiojo Teismo 2023 m. rugsėjo 12 d. nutartis civilinėje byloje Nr. e3K-3-182-1075/2023, 78 punktas.

susijusius personalizuotus saugumo duomenis mokėtojas privalo saugoti ir imtis visų reikiamų veiksmų, kad personalizuoti saugumo duomenys nebūtų atskleisti jokiems kitiems asmenims. Taisyklių 11 skyriuje įvardijama PIN kodų suvedimo reikšmė mokėjimo operacijų vykdymo procese ir jų panaudojimo galimos pasekmės mokėtojui⁷.

Banko ir pareiškėjos santykiams taip pat taikomas ir banko Paslaugų interneto banke teikimo sąlygų aprašas (toliau – Aprašas), kurio 20.4 papunktyje ir 38 punkte nurodyta, kad: „Klientas / naudotojas 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 / naudotojas privalo apie tai nedelsdamas pranešti teisėsaugos institucijoms. Už atpažinimo priemonių saugojimą ir tinkamą naudojimą, neatskleidimą tretiesiems asmenims yra atsakingas klientas; - Klientas / naudotojas įsipareigoja laikyti paslapyje 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.“

Taigi, pirmiau aptartos Taisyklių ir Aprašo nuostatos aiškiai ir nedviprasmiškai nustato tapatybės patvirtinimo priemonės personalizuotų saugumo duomenų naudojimo mokėjimo operacijų vykdymo procese paskirtį ir jų panaudojimo galimas pasekmes mokėtojui bei aiškiai ir nedviprasmiškai apibrėžia, kad už šių duomenų konfidencialumo išsaugojimą 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, jog pareiškėja ėmėsi pakankamų veiksmų (arba 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, o jai banko išduota mokėjimo priemonė būtų naudojama šalių sutartinius santykius reglamentuojančių dokumentų nustatyta tvarka bei sąlygomis.

Vertinant, ar pareiškėjos elgesys, kai ji suklustotoje Elektroninės valdžios vartų platformos sistemoje paspaudė nuorodą į banko interneto banko puslapį ir suvedė savo banko atpažinimo ir asmens kodus bei savo mobiliajame telefone suvedė „Smart-ID“ programėlės PIN1 kodą, taip patvirtindama trečiųjų asmenų prisijungimą prie savo interneto banko paskyros, o vėliau savo mobiliajame telefone suvedė „Smart-ID“ programėlės PIN2 kodą, taip patvirtindama ginčijamos mokėjimo operacijos įvykdymą, gali būti vertinamas kaip labai neatsargus, t. y. toks elgesys, dėl kurio mokėjimo priemonės turėtojo veiksmai iš esmės skiriasi nuo atsargaus elgesio reikalavimų, pažymėtina, kad įprastai panašaus pobūdžio ginčo byloje Lietuvos bankas vertina, kad vien tik faktas, jog mokėtojas paspaudžia jam trečiųjų asmenų atsiųstą aktyvią nuorodą ir nepastebi, kad patenka į suklustotą kokios nors bendrovės interneto puslapį, savaime nereiškia mokėtojo didelio neatsargumo. Paprastai sukčių pateiktos tiek pačios nuorodos į suklustotas bendrovių interneto svetaines, tiek ir pačios svetainės būna parengtos labai profesionaliai, dėl to vidutiniam vartotojui pagrįstai gali atrodyti, kad jis jungiasi prie tikros kokios nors bendrovės interneto svetainės.

Nagrinėjamo ginčo atveju iš pareiškėjos ir banko Lietuvos bankui pateiktų paaiškinimų galima teigti, kad sukčiavimo ataka nukreipta prieš pareiškėją buvo gerai parengta ir pareiškėjai, kaip vidutiniam vartotojui, pagrįstai galėjo atrodyti, kad Elektroninėje valdžios vartų platformoje paspausdama banko logotipą ji jungiasi prie savo interneto banko. Banko Lietuvos bankui pateikti duomenys patvirtina, kad bankas prieš pareiškėją suvedant „Smart-ID“ programėlės PIN1 kodą rodė pranešimą „Jungiatės prie SEB banko“. Taigi, pareiškėjai pagrįstai galėjo atrodyti, kad suveddama „Smart-ID“ programėlės PIN1 ji jungiasi prie savo interneto banko.

Tačiau, atkreiptinas dėmesys, kad panašaus pobūdžio sukčiavimo atakos nėra naujos ir visuomenėje gana plačiai žinomos, nes periodiškai skelbiama nemažai viešai prieinamos informacijos, įspėjančios vartotojus apie panašias sukčiavimo atakas ir raginančios juos būti budrius, nespaukti aktyvių nuorodų ir nevesti savo personalizuotų saugos duomenų.

Banko Lietuvos bankui pateiktais duomenimis, bankas pareiškėją asmeniškai jai siųstais elektroniniais laiškais informavo apie būdus, kuriais sukčiai gali mėginti pasisavinti iš banko sąskaitos pinigines lėšas, atkreipė pareiškėjos dėmesį į personalizuotų saugos duomenų mokėjimo operacijų vykdymo procese paskirtį ir galimas neatsargaus naudojimo pasekmes,

⁷ Banko pateiktais duomenimis, pareiškėja su Taisyklėmis ir jų naujausiais pakeitimais buvo asmeniškai supažindinta 2022 m. birželio 21 d. elektroniniu paštu siųstu pranešimu.

įspėjo pareiškėją nespausti jokių aktyvių nuorodų ir nesuvesti savo personalizuotų saugos duomenų.

Taigi, iš šių duomenų matyti, kad bankas prevenciškai dėjo pastangas tam, jog pareiškėja būtų supažindinta su sukčiavimo elektroninėje erdvėje rizikomis bei tapatybės patvirtinimo priemonės saugaus naudojimo, jos personalizuotų saugumo žymenų suvedimo ir atskleidimo reikšme bei teisinėmis pasekmėmis.

Vertinant tolesnius pareiškėjos veiksmus paspaudus aktyvią nuorodą ir patekus į trečiųjų asmenų suklastotą banko interneto banko puslapį, svarbu tai, kad pareiškėja tikėjosi, kaip ji pati paaiškino, prisijungti prie Elektroninės valdžios vartų sistemos. Tai reiškia, *kad pareiškėja neturėjo tikslo iš savo sąskaitos, panaudodama savo mokėjimo priemonės duomenis, įvykdyti mokėjimo operaciją*. Vis dėlto, ginčo byloje turimais duomenimis, pareiškėja ne tik suvedė savo personalizuotus saugos duomenis, reikalingus prisijungti prie savo interneto banko paskyros, bet ir suvedė „Smart-ID“ programėlės PIN2 kodą, tokiu būdu patvirtindama ginčijamos mokėjimo operacijos įvykdymą.

Pareiškėja teigė, kad prieš vesdama „Smart-ID“ programėlės PIN2 kodą ji nematė nei mokėjimo operacijos sumos, nei lėšų gavėjos duomenų. Tačiau banko Lietuvos bankui pateikti duomenys įrodo, kad prieš ginčijamos mokėjimo operacijos įvykdymą bankas pareiškėjai rodė tiek mokėjimo operacijos sumą, tiek ir lėšų gavėjos duomenis – *1 500 EUR i saskaita ****9865*. Taigi, pareiškėja, nors ir neturėdama tikslo iš savo banko sąskaitos įvykdyti mokėjimo operacijos, o turėdama tikslą tik prisijungti prie savo interneto banko paskyros, suvedė „Smart-ID“ programėlės PIN2 kodą ir taip patvirtino ginčijamos mokėjimo operacijos įvykdymą.

Taigi, pareiškėja, nors ir turėjo galimybę kritiškai įvertinti savo veiksmų su mokėjimo priemone riziką ir galimas pasekmes, nuo tolesnių veiksmų nesusilaikė, priešingai, vykdė visus trečiųjų asmenų nurodymus net nepaisydama to, kad bankas jai rodė tiek ginčijamos mokėjimo operacijos sumą, tiek ir lėšų gavėjo duomenis.

Kaip minėta, Taisyklių 1 priedo 11 skyriuje aiškiai reglamentuota, kad banko klientui suteiktų personalizuotų duomenų naudojimas yra skirtas duoti sutikimą įvykdyti mokėjimo operaciją. Ginčo byloje nėra duomenų, kad pareiškėja būtų buvusi nesupažindinta su Taisyklėmis ar kad būtų jų nesupratusi. Taigi, pareiškėja iš esmės galėjo suprasti, kad banko atpažinimo, asmens ir „Smart-ID“ paskyros PIN1 ir PIN2 kodų suvedimas gali lemti tam tikras teises pasekmes, šiuo atveju – mokėjimo priemonės praradimą ir neautorizuotos mokėjimo operacijos iš jos banko sąskaitos įvykdymą.

Įvertinus pirmiau nurodytas aplinkybes, Lietuvos banko nuomone, galima daryti išvadą, kad pareiškėja būtų galėjusi išvengti neautorizuotos mokėjimo operacijos iš savo sąskaitos įvykdymo, jeigu būtų buvusi pakankamai kritiška savo su mokėjimo priemone atliekamų veiksmų atžvilgiu ir būtų susilaikiusi nuo veiksmų su savo mokėjimo priemone. Pareiškėja turėjo galimybę suprasti, kad jos prašoma atlikti veiksmus, kuriais tvirtinamas mokėjimo operacijos įvykdymas, juolab kad bankas prieš ginčijamos mokėjimo operacijos įvykdymo patvirtinimą rodė tiek mokėjimo operacijos sumą, tiek lėšų gavėjo duomenis. Vis dėlto pareiškėja fakto, kad jos buvo prašoma suvesti „Smart-ID“ PIN2 kodą, nors ji pati ir nesiekė inicijuoti jokios mokėjimo operacijų, o tik norėjo prisijungti prie savo interneto banko paskyros, kai prisijungti prie interneto banko paskyros pakanka suvesti tik banko interneto banko atpažinimo, asmens ir „Smart-ID“ PIN1 kodus, nevertino kritiškai ir vykdė trečiųjų asmenų jai pateiktus nurodymus. Lietuvos banko vertinimu, toks pareiškėjos elgesys gali būti pripažintas kaip elgesys, iš esmės besiskiriantis nuo atsargaus elgesio reikalavimų, tai galiausiai ir lėmė, kad pareiškėja prarado savo mokėjimo priemonę, o tretieji asmenys įgijo galimybę jos vardu inicijuoti mokėjimo operaciją, kurią pareiškėja pati patvirtino suveddama „Smart-ID“ PIN2 kodą.

Taigi, įvertinus ginčo byloje turimus duomenis ir ginčo šalių paaiškinimus apie mokėjimo operacijų įvykdymo aplinkybes, galima teigti, kad pareiškėja mokėjimo priemone naudojosi nesilaikydama mokėjimo priemonės išdavimą ir naudojimą reglamentuojančių sąlygų ir neįvykdė Mokėjimų įstatymo 34 straipsnyje reglamentuojamų mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigų.

Visų ginčo byloje nustatytų aplinkybių kontekste galima daryti išvadą, kad pareiškėjos veiksmai, dėl kurių ji prarado mokėjimo priemonę, pasireiškė dideliu neatsargumu, tai galiausiai ir lėmė, jog buvo įvykdyta neautorizuota ginčijama mokėjimo operacija iš pareiškėjos sąskaitos ir pareiškėja patyrė nuostolių.

Mokėjimų įstatymo 39 straipsnio 3 dalyje nustatyta, kad mokėtojai 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.

Įvertinus pirmiau išdėstytą informaciją, konstatuotina, kad yra pagrindas pareiškėjai taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, todėl pareiškėjos reikalavimas bankui grąžinti neautorizuotos ginčijamos mokėjimo operacijos lėšų sumą yra nepagrįstas ir atmestinas.

2. *Dėl banke laikomų pareiškėjos lėšų saugumo*

Kaip minėta, nagrinėdamas ginčus Lietuvos bankas neatlieka patikrinimų tam, kad nustatytų, ar nebuvo pažeisti finansų įstaigų veiklai keliami teisės aktų reikalavimai. Lietuvos bankas remiasi ginčo šalių pateiktais konkrečiais įrodymais, kurių pagrindu priima sprendimą.

Vien tik pareiškėjos teiginiai, kad įvykdydamas ginčijamą mokėjimo operaciją, bankas neužtikrino mokėjimo operacijų stebėsenos, neturėjo rizikų valdymo sistemos, savaime nepagrindžia fakto, kad banko taikytos klientų lėšų apsaugos priemonės buvo nepakankamos ir (ar) neatitinkančios teisės aktų reikalavimų ir būtent tai galėjo nulemti, kad pareiškėja dėl mokėjimo operacijų įvykdymo patyrė nuostolių.

Be to, banko pateiktais duomenimis, bankas tą pačią dieną, kai gavo pareiškėjos pretenziją dėl neautorizuotos mokėjimo operacijos iš jos banko sąskaitos įvykdymo, kreipėsi į lėšų gavėjo mokėjimo paslaugų teikėją dėl lėšų grąžinimo, tačiau gavėjas lėšų nesugrąžino.

Duomenų, kad bankas būtų neįvykdęs ar netinkamai vykdęs finansų rinką reglamentuojančių teisės aktų reikalavimus ir (ar) nesiėmęs priemonių užtikrinti savo klientų, įskaitant pareiškėjos, banke laikomų lėšų saugumo, nagrinėjant ginčą nenustatyta.

Į esminius šalių išdėstytus argumentus atsakyta, o kiti šalių nurodyti argumentai neturi esminės reikšmės sprendimo teisėtumui ir pagrįstumui, todėl dėl jų Lietuvos bankas plačiau nepasisako. Lietuvos banko pareiga priimti motyvuotą sprendimą neturėtų būti suprantama kaip reikalavimas detaliai atsakyti į kiekvieną šalių argumentą⁸.

Remdamasis tuo, kas išdėstyta, ir vadovaudamasis Lietuvos Respublikos vartotojų teisių apsaugos įstatymo 27 straipsnio 1 dalies 3 punktu, Lietuvos banko valdybos 2012 m. sausio 26 d. nutarimo Nr. 03-23 „Dėl Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių patvirtinimo“ 2 punktu ir šiuo nutarimu patvirtintų Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių 59.3 papunkčiu, n u s p r e n d ž i u:

Atmesti pareiškėjos X.X. reikalavimą.

Lietuvos banko sprendimas dėl ginčo esmės yra rekomendacinio pobūdžio ir teismui neskundžiamas. Vartotojui ir finansų rinkos dalyviui išlieka teisė dėl tapataus ginčo dalyko kreiptis į teismą 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

⁸ Lietuvos Aukščiausiojo Teismo 2010 m. spalio 5 d. nutartis, priimta civilinėje byloje Nr. 3K-3-382/2010; 2010 m. gruodžio 20 d. nutartis civilinėje byloje Nr. 3K-3-536/2010 ir kt.