



**LIETUVOS BANKO
TEISĖS IR LICENCIJAVIMO DEPARTAMENTO
DIREKTORIUS**

**SPRENDIMAS
DĖL X. X. IR BANKO „SWEDBANK“, AB, GINČO NAGRINĖJIMO**

2026-01-14 Nr. 429-11
Vilnius

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

N u s t a t y t a:

2025 m. rugpjūčio 5 d. iš pareiškėjos banko sąskaitos, panaudojant tik pareiškėjai žinomus personalizuotus saugos duomenis, lėšų gavėjui Y.Y. (toliau – lėšų gavėjas) buvo atlikta 2 860 Eur mokėjimo operacija (toliau – ginčijama mokėjimo operacija).

Ginčo byloje nustatyta, kad pareiškėja socialiniame tinkle „Facebook“ rado skelbimą dėl nemokamo baseino. Susisiekus su asmeniu, jai buvo pasiūlyta pristatyti baseiną per DPD kurjerį už 8 Eur. Pareiškėja gavo aktyvią nuorodą į neva DPD interneto svetainę, joje pareiškėja suvedė savo duomenis, adresą, pasirinkusi banką, jos buvo paprašyta patvirtinti sumą pareiškėjos naudojamos atpažinimo priemonės mobiliojo parašo sPIN2 kodu.

Pareiškėjai paspaudus trečiųjų asmenų atsiųstą aktyvią nuorodą, joje atsidarė netikras interneto puslapis, imituojantis banko interneto puslapį, jame buvo prašoma įvesti tik pareiškėjai banko suteiktus ir žinomus personalizuotus saugos duomenis, reikalingus prisijungti prie interneto banko. Šiame netikrame puslapyje pareiškėja suvedė tiek duomenų, kiek jos buvo prašoma. Jie buvo reikalingi tretiesiems asmenims, kad jie iš savo įrenginio inicijuotų prisijungimą prie pareiškėjos interneto banko įprastos aplinkos, pradėtų jungimąsi per įsidiegtą banko išmaniają programėlę (toliau – Programėlę) ir susikurtų naują pareiškėjos tapatybės patvirtinimo priemonę – su savo įrenginio ekrano atrakinimo PIN kodu ar to įrenginio biometriniais duomenimis (toliau – Biometrika) savo įrenginyje. Kadangi pareiškėja suvedė prisijungimo duomenis ir savo mobiliajame įrenginyje prisijungimo veiksmą patvirtino pareiškėjos mobiliojo parašo sPIN2 kodu, tai leido tretiesiems asmenims susieti Programėlę, esančią trečiųjų asmenų mobiliajame įrenginyje, susieti su pareiškėjos tapatybe ir įgyti galimybę per įsidiegtą Programėlę naudojant tik tretiesiems asmenims žinoma Biometrika inicijuoti mokėjimo operacijas¹. Po šio veiksmo tretieji asmenys suformavo mokėjimo nurodymą įvykdyti ginčijamą mokėjimo operaciją, kuri viršijo sutartyje su banku numatytą mokėjimo limitą sumą, leidžiančią patvirtinti Biometrika, todėl pareiškėja gavo prašymą savo mobiliojo telefono mobilaus parašo programėlėje patvirtinti ginčijamą mokėjimo operaciją, ji tai ir padarė, suvesdama tik jai vienai žinomą sPIN2 kodą, ir ši operacija buvo įvykdyta.

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 lėšas, t. y. grąžinti 2 860 Eur. Pareiškėja Lietuvos bankui nurodė tapačias aplinkybes kaip ir bankui.

Pareiškėjos teigimu, ginčijama mokėjimo operacija iš jos banko sąskaitos buvo įvykdyta,

¹ Prieš suvesdama savo mobilaus parašo sPIN2 kodą svetimam įrenginiui patvirtinti, ji turėjo galimybę mobilaus parašo programėlėje susipažinti su informacija apie sutikimą, kurį jos prašoma duoti suvedant sPIN2 kodą: „Jungiatės su Samsung SM-S9310. Ar tai Jūsų įrenginys“.

nes banko taikomos lėšų apsaugos sistemos nėra pakankamos, bankas tinkamai nevykdė mokėjimo operacijų stebėsenos, nes ginčijama mokėjimo operacija akivaizdžiai neatitiko pareiškėjos mokėjimo įpročių.

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 jai atsiųstą netikrą interneto banko puslapį suvedė savo personalizuotus saugos duomenis, reikalingus prisijungti prie interneto banko paskyros, bei patvirtino ginčijamą mokėjimo operaciją savo mobilaus parašo sPIN2 kodu.

Be to, pareiškėja savo mokėjimo priemonę naudojo ne pagal paskirtį: pareiškėja, nesiekdama prisijungti prie savo interneto banko ir vykdyti jokių mokėjimo operacijų, suvedė savo mobiliojo parašo sPIN1 ir sPIN2 kodus, taip patvirtindama trečiųjų asmenų prisijungimą prie pareiškėjos interneto banko paskyros ir banko Programėlės įdiegimą trečiųjų asmenų įrenginyje, nors bankas, prieš suvedant minėtus duomenis, pareiškėjai jos mobiliojo telefono įrenginyje rodė informaciją apie veiksmą, kurį ji tvirtina. Banko vertinimu, tai, kad pareiškėja, veddama savo personalizuotus saugos duomenis, įskaitant ir mobiliojo parašo sPIN1 ir sPIN2 kodus, nors jai aiškiai buvo rodoma šių 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 inicijuoti ginčijamą mokėjimo operaciją, kurią patvirtino pati pareiškėja.

Bankas pažymėjo, kad ne tik tinkamai įvykdė ginčijamą mokėjimo operaciją, bet ir tinkamai suteikė ginčijamos mokėjimo operacijos atšaukimo paslaugą, tačiau ne dėl banko kaltės nepavyko sugrąžinti pareiškėjai ginčijamos mokėjimo operacijos lėšų.

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 ginčijamos mokėjimo operacijos ji nesiekė atlikti, o pareiškėjos personalizuotus saugumo duomenis tretieji asmenys gavo apgaulės būdu, bankas atsiliepime neginčija. Priešingai, bankas savo paaiškinimuose nurodo, kad dėl pareiškėjos 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, ar bankas: 1) atsisakydamas grąžinti pareiškėjai ginčijamos mokėjimo operacijos lėšas, pagrįstai rėmėsi Mokėjimų įstatymo 39 straipsnio 3 dalimi; 2) užtikrino lėšų pareiškėjos banko sąskaitoje saugumą.

1. Dėl banko atsisakymo grąžinti pareiškėjai ginčijamos mokėjimo operacijos 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 neautorizuotų mokėjimo operacijų įvykdymo, šiame sprendime atskirai nebus plačiau analizuojamas.

Taigi, sprendžiant, ar banko atsisakymas grąžinti pareiškėjai ginčijamų mokėjimo operacijų sumą laikytinas pagrįstu, būtina įvertinti, ar pareiškėjos elgesys, atskleidžiant tretiesiems asmenims personalizuotus saugumo duomenis, vertintinas kaip didelis neatsargumas, dėl kurio su mokėjimo operacijų 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 mokėtojai⁴.

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 tik šiais konkrečiais ginčo bylos aktualiais aspektais.

Neautorizuotų mokėjimo operacijų 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

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.

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, įgalino trečiuosius asmenis prisijungti prie interneto banko, o suveddama mobiliojo parašo SPIN2 kodą, leido tretiesiems asmenims susikurti naują su jos mokėjimo sąskaita susietą tapatybės patvirtinimo priemonę, t. y. trečiųjų asmenų įrenginyje įdiegtą Programėlę su Biometrika. Be to, pareiškėja, nors tokio veiksmo ir nesiekė atlikti, tačiau papildomai mobiliojo parašo SPIN2 kodu patvirtino ir ginčijamą mokėjimo operaciją. Banko teigimu, pareiškėjai prieš suvedant SPIN2 kodą buvo pateiktas informacinis pranešimas, kuriame buvo rodoma tvirtinamos ginčijamos mokėjimo operacijos informacija.

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 tretiesiems asmenims perimti savo sąskaitos valdymą ir šių veiksmų pagrindu tretieji asmenys galėjo inicijuoti ginčijamą mokėjimo operaciją, kurią pati pareiškėja net patvirtino, t. y. elgėsi itin aplaidžiai – buvo labai neatsargi.

Lietuvos bankas, siekdamas nustatyti, ar pareiškėjos elgesys šiuo atveju gali būti laikomas labai neatsargiu, vertino visų atliktų veiksmų visumą, t. y. jos elgesį paspaudžiant jai trečiųjų asmenų atsiųstą aktyvią nuorodą, suvedant savo mokėjimo priemonės personalizuotus saugumo duomenis suklustotame interneto banko puslapyje bei patvirtinant atliekamus veiksmus naudojama atpažinties priemone – suvedant savo mobiliojo parašo SPIN2 kodą, 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 iš trečiųjų asmenų gavo aktyvią nuorodą, kurią ji buvo skatinama paspausti ir suvesti savo personalizuotus saugos duomenis, kad apmokėtų kurjerio paslaugas. Kaip vėliau paaiškėjo, pareiškėja, paspaudusi trečiųjų asmenų jai atsiųstą aktyvią nuorodą, pateko į suklustotą interneto puslapį, jame suvedė tik jai žinomus asmeninius duomenis, šie buvo nusavinti trečiųjų asmenų (sukčių) ir panaudoti tam, kad būtų prisijungta prie pareiškėjos interneto banko paskyros ir kad trečiųjų asmenų įrenginyje būtų sukurta su pareiškėjos mokėjimo sąskaita susieta Programėlė su Biometrika. Pareiškėja tik jai žinomu SPIN2 kodu patvirtino tiek jai nežinomo naujo įrenginio naudojimą prisijungimui prie jos interneto banko aplinkos per naują su jos mokėjimo sąskaita susietą Programėlę ir jos Biometrikos sukūrimą, tiek vėliau pakartotinai SPIN2 kodu patvirtino mokėjimo operacijas (2795 Eur mokėjimo operaciją, kuri nebuvo įvykdyta, ir ginčijamą mokėjimo operaciją, kurios suma – 2860 Eur).

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

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

duomenys.

Banko ir pareiškėjos santykius reglamentuojančių banko Mokėjimo paslaugų teikimo taisyklių (toliau – Taisyklės) 22 punkte nustatyta, 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.

Banko ir pareiškėjos santykius reglamentuojančių banko Elektroninių paslaugų teikimo sutarties sąlygų (toliau – Sąlygos) 8 skyriuje reglamentuojama tapatybės patvirtinimo priemonės ir mokėjimo operacijų tvirtinimo ir (arba) pasirašymo procedūra, o 16 skyriuje nustatyta, kad banko suteiktą mokėjimo priemonę ir su ja susijusius personalizuotus saugumo duomenis mokėtojas privalo saugoti ir imtis visų reikiamų veiksmų, kad personalizuoti saugumo duomenys nebūtų atskleisti jokiems kitiems asmenims.

Taigi, pirmiau aptartos Taisyklių ir Sąlygų 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, gavusi trečiųjų asmenų aktyvią nuorodą į neva DPD puslapį, suklastotoje svetainėje suvedė savo asmeninius duomenis ir savo mobiliajame telefone suveddama savo mobiliojo parašo sPIN2 kodą patvirtino Programėlės susiejimą su pareiškėjos tapatybe trečiųjų asmenų įrenginyje, vėliau tuo pačiu sPIN2 kodu patvirtino ir pačią ginčijamą mokėjimo operaciją, 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 bylose Lietuvos bankas vertina, kad vien tik faktas, jog mokėtojas paspaudžia jam trečiųjų asmenų atsiųstą aktyvią nuorodą ir nepastebi, kad patenka į suklastotą kokios nors bendrovės interneto puslapį, savaime nereiškia mokėtojo didelio neatsargumo. Paprastai sukčių pateiktos tiek pačios nuorodos į suklastotas 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 prieš pareiškėją nukreipta sukčiavimo ataka buvo ne nauja, o gana plačiai žinoma, nes periodiškai skelbiama nemažai viešai prieinamos informacijos, įspėjančios vartotojus apie panašias sukčiavimo atakas ir raginančios juos būti budrius, nespausti aktyvių nuorodų ir nevesti savo personalizuotų saugos duomenų.

Banko Lietuvos bankui pateiktais duomenimis, bankas informaciją apie sukčiavimo atakas skelbė savo interneto banko puslapyje, SMS žinutėmis, be to, 2024 m. liepos 11 d. interneto banko žinute asmeniškai pareiškėjai priminė apie padažnėjusius sukčiavimo atvejus bei kaip atpažinti sukčiavimo veiksmus. Kaip minėta, nagrinėjamo ginčo situacijoje svarbu yra tai, kad pati sukčiavimo ataka, kai sukčiai ragina spausti neva siuntų pristatymo bendrovių nuorodas, turint tikslą už parduodamas prekes lėšas gauti į sąskaitą, yra plačiai žinoma visuomenėje, nes tiek bankai, tiek pačios siuntų pristatymo bendrovės, tiek skelbimų portalai, tiek ir kitos institucijos viešai įvairiais vartotojams prieinamais kanalais skelbia informaciją apie šį sukčiavimo būdą ir ragina nespausti aktyvių nuorodų ir nesusvesti savo mokėjimo priemonės duomenų, norint lėšas gauti į savo sąskaitą.

Atsižvelgiant į pirmiau minėtą informaciją, nėra pagrindo vertinti, kad, atsižvelgiant į sukčiavimo atakos pobūdį, pareiškėja neturėjo galimybių kritiškai įvertinti trečiųjų asmenų jai atsiųstos žinutės su aktyvia nuoroda ir susilaikyti nuo tolimesnių veiksmų.

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, sumokėti už norimos prekės (baseino) siuntimą 8 Eur, t. y. pareiškėja nesiekė susieti naujos Programėlės kaip savo tapatybės patvirtinimo priemonės kitame įrenginyje. Tačiau, ginčo byloje turimais duomenimis, pareiškėja ne tik suvedė savo

personalizuotus saugos duomenis, reikalingus prisijungti prie savo interneto banko paskyros, bet ir suvedė savo mobiliojo parašo SPIN2 kodą, taip patvirtindama trečiųjų asmenų prisijungimą prie jos banko sąskaitos bei Programėlės trečiųjų asmenų įrenginyje susiejimą su pareiškėjos mokėjimo sąskaita. Pareiškėja nekomentuoja, kodėl tris kartus suvedė savo SPIN2 kodą. Vis dėlto banko Lietuvos bankui pateikti duomenys įrodo, kad, prieš suveddama savo mobiliojo parašo SPIN2 kodą, kad nauja Programėlė būtų susieta su pareiškėjos mokėjimo sąskaita, pareiškėja turėjo galimybę mobilaus parašo programėlėje susipažinti su informacija apie sutikimą, kurį jos prašoma duoti suvedant SPIN2 kodą: „*Jungiatės su Samsung SM-S9310. Ar tai Jūsų įrenginys.*“ Be to, bankas du kartus siuntė pareiškėjos pasirinkto mobilaus parašo paslaugos teikėjui paklausimus dėl kredito pervedimų sąskaitoje patvirtinimo ir pareiškėja abu juos sėkmingai patvirtino savo SPIN2 kodu: pirma žinutė – „*2795 EUR pervesti gavėjui Y.Y. – patv*“; antra žinutė – „*2860 EUR pervesti gavėjui Y.Y. – patv*“.

Byloje turimais duomenimis, nors bankas įvykdė ginčijamą mokėjimo operaciją, tačiau iš banko pateiktų duomenų matyti, kad tretieji asmenys dar iki įvykdytos ginčijamos mokėjimo operacijos buvo iniciavę 2 795 Eur mokėjimo operaciją, kuri dėl viršyto limitu turėjo būti patvirtinta mobiliojo parašo SPIN2 kodu, tačiau ji buvo nesėkminga. Iš objektyvių duomenų matyti, kad pareiškėja 17:52:52 val. pradėjo jungtis iš savo įrenginio per Programėlę su savo įrenginio ekrano atrakinimo PIN kodu ar to įrenginio biometriniais duomenimis. Būtent šie veiksmai, t. y. prisijungimas prie Programėlės, užkirto kelią įvykdyti iniciuotą mokėjimo operaciją, nes pareiškėja savo veiksmais nutraukė mokėjimo operacijos patvirtinimo sesiją, kurią inicijavo tretieji asmenys iš savo išmanaus įrenginio per Programėlę, o pareiškėja jau net buvo patvirtinusi mobiliojo parašo SPIN2 kodu. Tai įvyko dėl to, nes vienu metu per Programėlę su Biometrika negalima būti prisijungus iš dviejų įrenginių. Taigi, tretieji asmenys turėjo prisijungti iš naujo, ir tai jiems pavyko 17:55 val.

Pakartotinai prisijungę tretieji asmenys vėl inicijavo mokėjimo nurodymo suformavimą, tačiau ginčijamos mokėjimo operacijos suma viršijo mokėjimo sumą, kurią bankas leidžia patvirtinti Biometrika, todėl pareiškėja vėl gavo prašymą savo mobiliojo telefono mobilaus parašo programėlėje patvirtinti ginčijamą mokėjimo operaciją. Tai ji padarė dar kartą suveddama SPIN2 kodą.

Svarbu pažymėti, kad banko pranešimų tekstas ir turinys, kuriuo pareiškėja buvo informuojama apie veiksmus, kurios tvirtina suveddama SPIN2 kodą, yra nedviprasmiškas ir informatyvus, t. y. aiškiai nurodoma konkreti mokėjimo operacijos suma, gavėjas ir tai, kad konkreti pinigų suma bus nurašyta iš banko sąskaitos. Iš banko prieš mokėjimo operacijos įvykdymo patvirtinimą pareiškėjai pateiktos informacijos galima teigti, kad rūpestingas ir atidus vartotojas turėjo visas galimybes pamatyti informaciją apie veiksmą, kurį tvirtina, ir susilaikyti nuo tolesnių veiksmų. Vis dėlto surinkti duomenys leidžia daryti išvadą, kad pareiškėja, prieš suveddama SPIN2 kodus, nekreipė deramo dėmesio į banko jai rodomą informaciją, suvedė SPIN2 kodus ir taip net du kartus patvirtino mokėjimo operacijų įvykdymą. Tik dėl atsitiktinumo pirmoji mokėjimo operacija nebuvo įvykdyta, o tik antroji ginčijama mokėjimo operacija buvo patvirtinta ir įvykdyta.

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, Sąlygų 8 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 Sąlygomis ar kad būtų jų nesupratusi. Be to, kaip paaiškino pati pareiškėja Lietuvos bankui, ji suprato, kad jungiasi prie savo banko sąskaitos, taip pat suprato, kad veddama SPIN2 kodą tvirtina mokėjimo operacijos vykdymą. Pareiškėja tik teigia, kad manė, jog atlieka 8 Eur mokėjimą.

Įvertinus pirmiau nurodytas aplinkybes, Lietuvos banko nuomone, galima daryti išvadą, kad pareiškėja būtų galėjusi išvengti neautorizuotos ginčijamos 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 prisijungimas prie banko sąskaitos bei Programėlės trečiųjų asmenų įrenginyje susiejimą su pareiškėjos mokėjimo sąskaita, kita vertus, pati pareiškėja nurodė, kad tikėjosi tik apmokėti siuntimo išlaidas – atlikti 8 Eur mokėjimo operaciją. Pareiškėja teigia supratusi, kad jos prašoma atlikti veiksmus, kuriais tvirtinamas mokėjimo operacijos įvykdymas, o bankas prieš

ginčijamos mokėjimo operacijos įvykdymo patvirtinimą aiškiai ir nedviprasmiškai rodė tiek mokėjimo operacijos sumą, tiek lėšų gavėjo duomenis. Vis dėlto pareiškėja į šią banko rodytą informaciją nekreipė deramo dėmesio ir vykdė trečiųjų asmenų jai pateiktus nurodymus, tai ir lėmė, kad iš pareiškėjos banko sąskaitos buvo įvykdyta ginčijama mokėjimo operacija. Be to, pareiškėja fakto, kad jos buvo prašoma suvesti mobiliojo parašo SPIN2 kodą, nors ji pati ir nesiekė prisijungti prie savo interneto banko paskyros arba įdiegti banko Programėlės, 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 operacijas, pareiškėjai patvirtinus Programėlės trečiųjų asmenų įrenginyje susiejimą su pareiškėjos mokėjimo sąskaita.

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 neautorizuotos 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 lėšas 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 operacijos įvykdymo patyrė nuostolių.

Duomenų, kad bankas būtų nevykdęs 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 argumentą⁷.

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

⁷ 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.

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