



**LIETUVOS BANKO
TEISĖS IR LICENCIJAVIMO DEPARTAMENTO
DIREKTORIUS**

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

2025-11-04 Nr. 429-268
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 18 d. iš pareiškėjos banko sąskaitos, panaudojant tik pareiškėjai žinomus personalizuotus saugos duomenis, lėšų gavėjui *duomenys neskelbiami* (toliau – lėšų gavėjas) buvo atlikta 1 100 Eur mokėjimo operacija (toliau – ginčijama mokėjimo operacija).

Ginčo byloje nustatyta, kad pareiškėja, turėdama tikslą prisijungti prie AB „Lietuvos draudimas“ interneto svetainės, *Google* paieškos sistemoje suvedė reikšminius žodžius *Lietuvos draudimas*, pateko į minėtos bendrovės suklastotą puslapį ir paspaudė banko logotipą, turėdama tikslą patvirtinti savo tapatybę. 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 kodus. Taip pat pareiškėja prisijungimą turėjo patvirtinti jos 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. Ginčijamos mokėjimo operacijos įvykdymas buvo patvirtintas tik vienai pareiškėjai žinomu „Smart-ID“ PIN2 kodu.

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 1 100 Eur. Pareiškėja Lietuvos bankui paaiškino, kad „2025-08-18 dieną man bandant prisijungti prie Lietuvos draudimo savitarnos mane nukreipė į netikrą nuorodą, kuri buvo su LD logo ir identišku interfeisu, prašant patvirtinti tapatybę su vienu iš pasirinktų bankų pasirinkau swedbank su SmartID, išmetus pin kodo prašymą patvirtinau kodu ir iškart gavau pranešimą, kad nuo mano sąskaitos nurašyta 1100eur suma gavėjui Mariusz.“

Pareiškėja teigia „Smart-ID“ paskyros PIN1 kodu tvirtinusi tik savo prisijungimą prie interneto banko, o bankas jai nerodė jokios informacijos, susijusios su mokėjimo operacijos suma bei gavėju. Vis dėlto telefoninio pokalbio metu pareiškėja teigė, kad ji suvedė „Smart-ID“ PIN2 kodą, norėdama sumokėti už draudimo paslaugas, tačiau bankas jai nerodė nei ginčijamos mokėjimo operacijos sumos, nei gavėjo duomenų.

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 pareiškėja, prieš suvedama „Smart-ID“ PIN1 ir PIN2 kodus, nekreipė dėmesio į banko jai rodomą informaciją.

Bankas paaiškino, kad, jo turimais sistemų duomenimis, pareiškėja, prieš suvedama „Smart-ID“ PIN1 kodą, turėjo galimybę matyti, kad tvirtina prisijungimą prie banko interneto banko, nes jos telefone atsidariusiame „Smart-ID“ programėlės ekrane buvo pateiktas tokio turinio teksto pranešimas - „Prisijungiate prie Swedbank interneto banko“.

Bankas paaiškino, kad net jeigu pareiškėja galėjo manyti, kad ji, o ne tretieji asmenys,

jungiasi prie savo interneto banko paskyros, pareiškėjai suvedus „Smart-ID“ PIN1 kodą, lėšos pareiškėjos banko sąskaitoje dar buvo saugios.

Banko turimų sistemų duomenimis, tretieji asmenys prisijungė prie pareiškėjos interneto banko ir inicijavo ginčijamos mokėjimo operacijos įvykdymą, o sutikimą įvykdyti šią mokėjimo operaciją davė pati pareiškėja, suvedama „Smart-ID“ PIN2 kodą. Bankas, prieš pareiškėjai vedant „Smart-ID“ PIN2 kodą, jos mobiliojo telefono ekrane aiškiai ir nedviprasmiškai rodė tiek ginčijamos mokėjimo operacijos sumą, tiek ir gavėjo duomenis: „Pervedimas 1 100 EUR - patvirtinkite ir lėšos bus nurašytos nuo Jūsų sąskaitos. Jūsų nurodytas lėšų gavėjas: Mariusz Ja Skobel.“

Banko teigimu, pareiškėja turėjo visas galimybes perskaityti išsamią ir nedviprasmišką informaciją apie veiksmą, kuriam jos prašoma duoti sutikimą ir susilaikyti nuo tolimesnių veiksmų, tačiau ji pasirinko mygtuką „Patvirtinti“ ir suvedė „Smart-ID“ PIN2 kodą.

Banko vertinimu, tai, kad pareiškėja, vedama 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 ginčijamos mokėjimo operacijos įvykdymo bankas pareiškėją buvo informavęs apie sukčiavimo grėsmes naudojantis mokėjimo paslaugomis¹. Taip pat, banko teigimu, jau keletą metų viešoje erdvėje skelbiama daug informacijos apie sukčiavimo atakas ir teikiami patarimai vartotojams būti budriems.

Be to, bankas paaiškino, kad nuo 2025 m. birželio mėn. prieš kiekvienos mokėjimo operacijos įvykdymą savo paslaugų vartotojus, įkaitant ir pareiškėją, įspėjantis saugotis sukčiavimo.

Papildomai bankas pažymėjo, kad, gavęs pareiškėjos pretenziją dėl neautorizuotos mokėjimo operacijos įvykdymo, nedelsdamas 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 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 jai nepateikė informacijos apie mokėjimo operacijos sumą bei gavėją. Banko teigimu, pareiškėjos veiksmams 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. birželio 21 d.

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, atsisakydamas grąžinti pareiškėjai ginčijamos mokėjimo operacijos metu pervestas lėšas, pagrįstai rėmėsi Mokėjimų įstatymo 39 straipsnio 3 dalimi.

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, kai 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 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

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.

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, suveddama „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 AB „Lietuvos draudimas“ svetainės, 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 galimai suklustotos AB „Lietuvos draudimas“ interneto svetainės, prisijungusi paspaudė banko logotipą, pateko į suklustotą banko interneto banko puslapį, kuriame suvedė prašomus nurodyti duomenis: banko atpažinimo ir asmens kodus. Šie duomenys, 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 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 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 Elektroninių paslaugų teikimo sąlygų

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

(toliau – Sąlygos) 6 punkte reglamentuojama tapatybės patvirtinimo priemonės ir mokėjimo operacijų tvirtinimo ir (arba) pasirašymo procedūra. Sąlygų 6.1 papunktyje aiškiai nurodomi mokėjimo operacijų pasirašymo bei tvirtinimo būdai: „elektroniniu parašu, kuris yra generuojamas panaudojant kodus nurodytus Banko išduotame PIN generatoriuje ar kitose Banko išduotose priemonėse, arba jų kombinacijas kaip nurodyta 6.1.4 p.; arba Bankui priimtinu pažangiuoju elektroniniu parašu; arba Bankui priimtinu kvalifikuotu elektroniniu parašu; arba naudojant kitas Bankui priimtinas alternatyvias autorizavimo procedūras, kai Naudotojas savo valią išreiškia panaudodamas nuolatinį slaptažodį, slaptažodžius, SMS žinute siunčiamus kodus, unikalius mobilaus telefono aparato duomenis, mobilaus telefono numerį, išmaniajame įrenginyje nuskaitytus ir / ar išsaugotus biometrinius duomenis ir pan. arba šiame 6.1 punkte nurodytų būdų kombinacijomis.“

Taigi, pirmiau aptartos Taisyklių ir Sąlygų nuostatos aiškiai nustato tapatybės patvirtinimo priemonės personalizuotų saugumo duomenų naudojimo mokėjimo operacijų vykdymo procese paskirtį ir jų panaudojimo galimas pasekmes mokėtojui, 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 AB „Lietuvos draudimas“ svetainėje paspaudė nuorodą į suklustotą 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 bylose 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 vidutinei vartotojai, pagrįstai galėjo atrodyti, kad suklustotoje AB „Lietuvos draudimas“ svetainėje, paspausdama banko logotipą, ji jungiasi prie savo interneto banko.

Banko Lietuvos bankui pateikti duomenys patvirtina, kad bankas prieš pareiškėjai suvedant „Smart-ID“ programėlės PIN1 kodą rodė pranešimą „Prisijungiate prie Swedbank interneto banko“. Taigi, pareiškėjai pagrįstai galėjo atrodyti, kad suvedama „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 atkas ir raginančios juos būti budrius naudojant savo personalizuotus saugos duomenis.

Banko Lietuvos bankui pateiktais duomenimis, bankas pareiškėją asmeniškai jai siųstu elektroniniu laišku 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. Be to, bankas ir prieš mokėjimo operacijos įvykdymą, pateikė pranešimą, įspėjantį apie sukčiavimo riziką, ir įspėjo būti atsargią naudojant savo mokėjimo priemonę.

Taigi, iš šių duomenų matyti, kad bankas prevenciškai dėjo pastangas tam, kad 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 AB „Lietuvos draudimas“ svetainės. Papildomai telefonu pareiškėja paaiškino, kad prisijungusi prie AB „Lietuvos draudimas“ svetainės ji norėjo sumokėti už draudimo paslaugas.

Nors pareiškėja teigia, kad bankas jai, prieš suvedant „Smart-ID“ programėlės PIN2 kodą, nerodė informacijos nei apie sumą, nei apie gavėją, 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: *„Patvirtinkite informaciją. Norėdami tęsti, įsitikinkite, kad jūsų operacijos informacija yra teisinga. 'Pervedimas 1 100 EUR - patvirtinkite ir lėšos bus nurašytos nuo Jūsų sąskaitos. Jūsų nurodytas lėšų gavėjas: Mariusz Ja Skobel“*.

Svarbu pažymėti, kad banko pranešimo tekstas turinys, kuriuo pareiškėja buvo informuojama apie veiksmą, kurį tvirtina suvedama „Smart-ID“ programėlės PIN2 kodą, yra nedviprasmiškas ir informatyvus, t. y. jame 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 tolimesnių veiksmų. Vis dėlto ginčo byloje surinkti duomenys leidžia daryti išvadą, kad pareiškėja prieš suvedama „Smart-ID“ programėlės PIN2 kodą nekreipė deramo dėmesio į banko jai rodomą informaciją, suvedė „Smart-ID“ programėlės PIN2 kodą ir taip patvirtino ginčijamos mokėjimo operacijos įvykdymą.

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 6 punkte 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 pati pareiškėja Lietuvos bankui paaiškino, ji suprato, kad, vedama savo banko atpažinimo, asmens ir „Smart-ID“ paskyros PIN1 kodus, ji jungiasi prie savo banko sąskaitos, taip pat suprato, kad vedama „Smart-ID“ paskyros PIN2 kodą tvirtina mokėjimo operacijos įvykdymą. Pareiškėja tik teigia, kad bankas jai nerodė nei mokėjimo operacijos sumos, nei gavėjo.

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 atidi ir kritiška savo su mokėjimo priemone atliekamų veiksmų atžvilgiu ir būtų susilaikiusi nuo veiksmų su savo mokėjimo priemone. Pareiškėja, kaip ji pati teigia, suprato, 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 prieš mokėjimo operacijos įvykdymą rodytą informaciją nekreipė deramo dėmesio ir vykdė trečiųjų asmenų jai pateiktus nurodymus, kas ir lėmė, kad iš pareiškėjos banko sąskaitos buvo įvykdyta ginčijama mokėjimo operacija.

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 suvedama „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.

Be to, bankas, gavęs pareiškėjos pretenziją dėl neautorizuotos mokėjimo operacijos įvykdymo, nedelsdamas kreipėsi į lėšų gavėjo banką, tačiau lėšų sugrąžinti nepavyko.

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.

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 detalai 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 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

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.