LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

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

2024-02-21 Nr. 429-32
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:

2023 m. gruodžio 8 d. 17 val. 55 min. iš pareiškėjos atsiskaitomosios sąskaitos banke buvo atlikta 2 000 Eur mokėjimo operacija gavėjai Y. Y. (toliau – Operacija).

Tą pačią dieną 19 val. 20 min. pareiškėja kreipėsi telefonu į banką ir pranešė, kad socialiniame tinkle „Facebook“ paskelbė informaciją apie parduodamą prekę. Pareiškėja nurodė, kad dėl prekės į ją kreipėsi tretieji asmenys. Pareiškėja per mobiliąją pokalbių programėlę „Messenger“ gavo nepažįstamo pirkėju prisistačiusio asmens žinutę, kad jis siekia įsigyti parduodamą prekę pagal įkeltą skelbimą. Pareiškėjos teigimu, pirkėju prisistatęs asmuo vėliau atsiuntė ir nuorodą į siuntų pristatymo bendrovės „DPD“ interneto svetainę, kurioje turėjo būti suvesti pareiškėjos personalizuoti saugumo duomenys tam, kad tariamo pirkėjo pervesta suma už parduodamą prekę būtų įskaityta į pareiškėjos sąskaitą banke. Pareiškėja nurodė, kad paspaudė gautą aktyvią nuorodą, suvedė prisijungimo prie banko sąskaitos identifikacinį numerį ir vieną kodų generatoriaus sugeneruotą kodą (APPLI1). Po šių veiksmų pareiškėja teigia iš karto gavusi pranešimą, kad iš jos sąskaitos buvo nurašytos lėšos.

Pokalbio metu pareiškėjai teikiama interneto banko paslauga buvo užblokuota, o pareiškėjai buvo rekomenduota pateikti prašymą atšaukti pervedimą.

2023 m. gruodžio 8 d. 19 val. 40 min. pareiškėja pateikė prašymą atšaukti pervedimą.

Atsižvelgdamas į pareiškėjos pateiktus duomenis, bankas nustatė, kad nėra techninių galimybių atšaukti Operaciją. Dėl šios priežasties, remdamasis visa surinkta informacija, bankas priėmė sprendimą atsisakyti pareiškėjai atlyginti jos patirtus nuostolius, nes nustatė, kad pareiškėja pati, būdama labai neatsargi, perdavė tretiesiems asmenims personalizuotus saugumo duomenis, pasinaudojus šiais duomenimis buvo patvirtinta Operacija, todėl bankas neprivalo savo lėšomis padengti pareiškėjos patirtų nuostolių.

Pareiškėja kreipėsi į banką ir prašė pakartotinai apsvarstyti priimtą sprendimą, tačiau bankas pareiškėjai pateikė atsakymą, kad priimtas sprendimas yra pagrįstas ir keičiamas nebus. Pareiškėja su tuo nesutiko, todėl tarp šalių kilo ginčas.

Kreipimesi į Lietuvos banką pareiškėja prašo įvertinti banko veiksmus ir įpareigoti banką grąžinti Operacijos metu iš pareiškėjos atsiskaitomosios sąskaitos nurašytas lėšas, t. y. 2 000 Eur. Pareiškėja Lietuvos bankui nurodė analogiškas faktines aplinkybes kaip ir kreipimesi į banką. Pareiškėja papildomai pažymėjo, kad neketino atlikti jokios mokėjimo operacijos, neįvedė kodų generatoriaus APPLI2 kodo, t. y. nepatvirtino Operacijos, nespaudė jokių papildomų mygtukų, kad būtų inicijuota mokėjimo operacija. Pareiškėja nurodo, kad bankas pažeidė jos teises ir teisėtus interesus, todėl turi grąžinti pareiškėjos prarastas lėšas.

Atsiliepime į pareiškėjos kreipimąsi bankas nurodo nesutinkąs su pareiškėjos reikalavimu ir prašo jį atmesti. Banko teigimu, pareiškėja dėl savo didelio neatsargumo neišsaugojo savo personalizuotų saugos duomenų, dėl to tretieji asmenys jais galėjo pasinaudoti ir be pareiškėjos žinios inicijuoti ir patvirtinti Operaciją.

Banko teigimu, pareiškėja atsidariusiame suklastotame banko interneto banko puslapyje pateikė savo asmeninius prisijungimo prie interneto banko duomenis, tada kodų generatoriuje turėjo suvesti APPLI1 kodą ir taip leisti tretiesiems asmenims prisijungti prie savo banko

sąskaitos. Bankas pažymi, kad nors pareiškėja nurodo tik vieną kartą suvedusi kodų generatoriaus APPLI1 kodą, tačiau iš banko turimų objektyvių duomenų matyti, kad pareiškėja turėjo atlikti aktyvius veiksmus tam, kad sužinotų APPLI2 kodą ir jį perduotų tretiesiems asmenims, o šie jį suvedė ir taip patvirtino Operaciją. Be to, banko teigimu, pareiškėja iki Operacijos autorizavimo ne kartą buvo prisijungusi prie savo interneto banko paskyros iš savo įrenginio, todėl jai buvo sudarytos visos sąlygos prieš suvedant kodų generatoriaus APPLI2 kodą susipažinti su Operacijos detalėmis ir priimti tinkamą sprendimą – neperduoti tretiesiems asmenims kodų generatoriuje suformuoto kodo.

Banko teigimu, apie sukčių vykdomas atakas ir bandymus išvilioti lėšas bankas nuolatos skelbia žiniasklaidoje ir kitomis priemonėmis. Bankas reguliariai įspėja klientus apie sukčiavimo atvejus, o 2022 m. rugpjūčio 25 d. interneto banko žinute pareiškėjai siuntė naudingą informaciją, kaip apsisaugoti nuo sukčių.

Bankas nurodo, kad pareiškėjai būtų pavykę išvengti dėl Operacijos kilusių nuostolių, jei tik ji būtų neskubėjusi ir atidžiai įvertinusi nepažįstamo trečiojo asmens atsiųstą pranešimą ir jame pateiktą aktyvią nuorodą bei aplinkybę, ar tapatybei patvirtinti siekiant gauti lėšas į sąskaitą turi būti suformuojamas ir įvedamas kodų generatoriaus APPLI2 kodas.

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 45 punktu, vartojimo ginčai Lietuvos banke nagrinėjami laikantis rungimosi, ginčų nagrinėjimo operatyvumo, koncentracijos, ekonomiškumo ir bendradarbiavimo principų. Vartotojas ir finansų rinkos dalyvis privalo įrodyti tas aplinkybes, kuriomis remiasi kaip savo reikalavimų arba atsikirtimų pagrindu, išskyrus atvejus, kai remiamasi aplinkybėmis, kurių nereikia įrodinėti. Nagrinėdamas ginčą Lietuvos bankas atlieka ginčo šalių pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Pareiškėjos ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjai Operacijos metu iš jos atsiskaitomosios sąskaitos banke pervestą sumą. Pareiškėja neigia autorizavusi Operaciją, todėl mano, kad bankas Operacijos lėšas turi grąžinti pareiškėjai. Banko vertinimu, pareiškėjos veiksmams būdingas didelis neatsargumas, todėl bankas negali būti įpareigotas Operacijos sumos grąžinti pareiškėjai.

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 Operacija nėra pareiškėjos autorizuota, o pareiškėjos personalizuotus saugumo duomenis ir pareiškėjos sutikimą tretieji asmenys gavo apgaulės būdu, bankas atsiliepime neginčija. Priešingai, bankas savo paaiškinimuose nurodo, kad dėl pareiškėjos atskleistų duomenų tretieji asmenys įgijo galimybę inicijuoti ir patvirtinti Operaciją. Dėl šios priežasties yra akivaizdu, kad Operacijos inicijavimas ir patvirtinimas neatitiko pačios pareiškėjos valios, nors formaliai (pagal išorinius požymius) ir sutapo su pareiškėjos ir banko sutarta sutikimo atlikti mokėjimo operacijas davimo forma ir tvarka. Atsižvelgdamas į tai, Lietuvos bankas daro išvadą, kad Operacija, atlikta nesant pareiškėjos valios ir jai net nežinant apie Operacijos inicijavimo aplinkybę bei neišreiškus jokių valinių veiksmų patvirtinti Operaciją, laikytina neautorizuota.

Siekdamas išspręsti tarp šalių kilusį ginčą ir įvertinti pareiškėjos bankui keliamo reikalavimo pagrįstumą, Lietuvos bankas vertins, ar atsisakydamas grąžinti pareiškėjai Operacijos metu pervestas lėšas bankas pagrįstai rėmėsi Mokėjimų įstatymo 39 straipsnio 3 dalimi.

Mokėjimų įstatymo 39 straipsnio 3 dalyje nustatyta, kad mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai, jeigu jis juos patyrė veikdamas

nesąžiningai arba tyčia ar dėl didelio neatsargumo neįvykdęs vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų.

Taip pat svarbu pažymėti, kad Lietuvos Aukščiausiasis Teismas yra konstatavęs, kad 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. Jeigu 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 sąlyga[1].

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 mokėtojui nuostolius dėl neautorizuotos mokėjimo operacijos įvykdymo, šiame sprendime atskirai nebus plačiau analizuojamas.

Taigi, sprendžiant, ar banko atsisakymas grąžinti pareiškėjai 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 aplinkybėmis[2]. 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 mokėtojui[3].

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 praktikoje[4], 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 mokėtojui 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 kad tai padarė dėl didelio neatsargumo[5].

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 Operacijos pareiškėja patyrė dėl savo didelio

---

[1] Lietuvos Aukščiausiojo Teismo 2023 m. rugsėjo 12 d. nutartis civilinėje byloje Nr. e3K-3-182-1075/2023, 44 punktas.
[2] Lietuvos Aukščiausiojo Teismo 2017 m. balandžio 13 d. nutartis civilinėje byloje Nr. e3K-3-180-378/2017.
[3] Lietuvos Aukščiausiojo Teismo 2023 m. rugsėjo 12 d. nutartis civilinėje byloje Nr. e3K-3-182-1075/2023, 82 punktas.
[4] Pavyzdžiui, ginčo bylos Nr. 2022-00586 ir 2022-02496.
[5] Lietuvos Aukščiausiojo Teismo 2023 m. rugsėjo 12 d. nutartis civilinėje byloje Nr. e3K-3-182-1075/2023, 78 punktas.

neatsargumo, t. y. pareiškėja, perduodama tretiesiems asmenims savo personalizuotus saugumo duomenis, suvesdama kodų generatoriaus APPLI1 kodą ir taip leisdama tretiesiems asmenims prisijungti prie pareiškėjos banko paskyros ir perduodama tretiesiems asmenims kodų generatoriaus APLLI2 kodą, suteikė leidimą tretiesiems asmenims inicijuoti ir atlikti Operaciją pareiškėjos vardu.

Lietuvos bankas neturi pakankamai patikimų įrodymų, galinčių patvirtinti arba paneigti banko teiginius, kad būtent pareiškėja tretiesiems asmenims atskleidė kodų generatoriaus sugeneruotą APPLI2 kodą, o pareiškėja tiek kreipimesi į banką, tiek ir į Lietuvos banką tokias aplinkybes neigia. Tačiau, Lietuvos banko vertinimu, svarbu pažymėti, kad be kodų generatoriaus APPLI2 kodo nagrinėjamu atveju nebūtų buvę galima tinkamai patvirtinti Operaciją. Tiek iš pareiškėjos, tiek iš banko pateiktų duomenų matyti, kad pareiškėja nebuvo pranešusi, kad jos turimas kodų generatorius būtų buvęs pamestas ar pasisavintas trečiųjų asmenų. Bankas taip pat pateikė objektyvius duomenis, t. y. savo sistemų išrašus, kuriuose matyti, kad Operacija buvo patvirtinta pareiškėjos kodų generatoriaus sugeneruotu kodu[6]. Dėl šių aplinkybių nagrinėjamu atveju labiau tikėtina, kad pati pareiškėja turėjo tretiesiems asmenims perduoti jos kodų generatoriaus sugeneruotą APPLI2 kodą, kuriuo tretieji asmenys patvirtino Operaciją.

Lietuvos bankas, siekdamas nustatyti, ar pareiškėjos elgesys šiuo atveju gali būti laikomas dideliu neatsargumu, vertino pareiškėjos elgesį pasitikint pokalbių programėlėje gautame pranešime nurodyta informacija ir spaudžiant joje pateiktą nuorodą, suvedant pareiškėjos mokėjimo priemonės personalizuotus saugumo duomenis suklastotame interneto puslapyje bei patvirtinant atliekamus veiksmus (savo tapatybę) kodų generatoriumi – suvedant APPLI1 kodą bei perduodant APPLI2 sugeneruotą kodą tretiesiems asmenims, taip pat kokių prevencijos veiksmų ėmėsi ir imasi bankas 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 Operaciją.

Lietuvos bankas, įvertinęs pareiškėjos kreipimesi ir banko atsiliepime nurodytas aplinkybes bei kartu su kreipimusi ir atsiliepimu pateiktus duomenis, nustatė, kad prieš Operacijos įvykdymą pareiškėja pokalbių programėlėje „Messenger" gavo, kaip tuo metu buvo tikima, pirkėjo siųstą pranešimą apie siuntų bendrovės „DPD" sistemoje apmokėtą parduodamą prekę, paspaudė pranešime pateiktą nuorodą ir suklastotame „DPD" puslapyje suvedė prašomus prisijungimo prie banko sąskaitos duomenis, kurie, kaip paaiškėjo vėliau, buvo nusavinti trečiųjų asmenų (sukčių) ir panaudoti tam, kad būtų prisijungta prie pareiškėjos internetinės banko sąskaitos ir inicijuota Operacija.

Pareiškėjos bendrąją sutartį sudarančių banko mokėjimo paslaugų teikimo sąlygų[7] 7.1 papunktyje, reglamentuojančiame su mokėjimo priemone susijusias banko kliento pareigas, nustatyta, kad: „7.1.1. Klientas, turintis teisę naudotis Mokėjimo priemone, privalo: 7.1.1.1. naudotis Mokėjimo priemone pagal Mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, nurodytas atitinkamoje Sutartyje ir/ar Paslaugos sąlygose; 7.1.1.2. sužinojęs apie Mokėjimo priemonės vagystę ar praradimą kitu būdu, įtarus ar sužinojus apie Mokėjimo priemonės neteisėtą įgijimą arba neautorizuotą jos naudojimą, taip pat apie faktus ar įtarimus, kad Mokėjimo priemonės personalizuotus saugumo duomenis (įskaitant Tapatybės patvirtinimo priemones) sužinojo arba jais gali pasinaudoti Tretieji asmenys, nedelsdamas apie tai pranešti Bankui ar kitam jo nurodytam subjektui, vadovaujantis Mokėjimo priemonės išdavimą ir naudojimą reglamentuojančiomis sąlygomis, nurodytomis Sutartyje ir/ar Paslaugos sąlygose. 7.1.2. Klientas, gavęs Mokėjimo priemonę, privalo iš karto imtis visų veiksmų (įskaitant nurodytus Paslaugos sąlygose ir atitinkamoje Sutartyje), kad būtų apsaugoti gautos Mokėjimo priemonės personalizuoti saugumo duomenys (įskaitant Tapatybės patvirtinimo priemones)." Be to, vadovaujantis banko viešai skelbiamomis saugaus naudojimosi elektroninėmis paslaugomis rekomendacijomis, banko klientai raginami nespausti jokių el. paštu, pokalbių programėlėse ar SMS žinutėse gautų nuorodų, nevykdyti prašymų suvesti arba padiktuoti prisijungimo prie interneto banko ar kortelės duomenis, atidžiai įvertinti savo telefono ekrane matomą prašymą įvesti turimos prisijungimo priemonės slaptažodį, jei nėra su

[6] Iš banko pateiktų duomenų matyti, kad kodų generatoriaus APPLI2 parodymai buvo 52346323, o kodų generatorius sugeneravo 71149026 APPLI2 kodą.
[7] https://www.swedbank.lt/static/pdf/legalisation/business/mokejimu_paslaugu_teikimo_salygos_2023-10-01.pdf

kuo sulyginti kontrolinio kodo arba jis nesutampa, arba ignoruoti tokį pranešimą, jei nesiekiama prisijungti prie interneto banko ar inicijuoti mokėjimo operacijų, kilus nors mažiausiai abejonei, neskubėti ir nedelsiant nutraukti veiksmus.

Taigi, pirmiau aptartos mokėjimo paslaugų sutarties (ją sudarančių dokumentų) nuostatos aiškiai nustato, kad už mokėjimo ir tapatybės patvirtinimo priemonių personalizuotų saugumo duomenų konfidencialumą yra atsakingas mokėtojas, šiuo atveju – pareiškėja, ji privalo užtikrinti, kad minėti duomenys netaptų žinomi tretiesiems asmenims. Atsižvelgiant į tai, manytina, kad pareiškėjos elgesys būtų laikomas kaip atitinkantis mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, jei būtų nustatyta, kad pareiškėja ėmėsi adekvačių veiksmų (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 ir jie būtų naudojami šalių sutartinius santykius reglamentuojančių dokumentų nustatyta tvarka bei sąlygomis.

Vis dėlto, įvertinus ginčo byloje esančius duomenis ir ginčo nagrinėjimo metu nustatytas aplinkybes, išvados, kad pareiškėjos elgesys atitiko banko nustatytas naudojimosi mokėjimo priemonėmis sąlygas ir buvo adekvatus, pakankamas tam, kad pareiškėjai nustatytos pareigos, susijusios su mokėjimo priemonių personalizuotų saugumo duomenų konfidencialumo užtikrinimu, būtų tinkamai įvykdytos, daryti negalima.

Nors pareiškėjai į pokalbių programėlę atsiųstas nepažįstamo asmens (tariamo pirkėjo) pranešimas galėjo sukurti pirminį įspūdį, kad šis pranešimas išsiųstas potencialaus pirkėjo, tačiau tai, kad pareiškėja iki personalizuotų duomenų atskleidimo (pateikimo suklastotoje interneto svetainėje) nesudvejojo pranešime nurodytos informacijos ir nepažįstamo siuntėjo patikimumu, leidžia teigti, kad pareiškėjos elgesys, suteikiant tretiesiems asmenims personalizuotus saugumo duomenis, suteikė galimybę tretiesiems asmenims prisijungti prie pareiškėjos banko programėlės ir inicijuoti Operaciją, todėl jis nebuvo itin apdairus ir atsargus.

Svarbu pažymėti, kad trečiųjų asmenų pareiškėjai atsiųsta nuoroda https://dpd.ordertrustpay.site/pay/order/QViBMxjM akivaizdžiai skyrėsi nuo tikros bendrovės „DPD" interneto svetainės nuorodos (tikra svetainės nuoroda https://www.dpd.com/lt/lt/). Taigi, Lietuvos banko nuomone, pareiškėja galėjo suprasti, kad pateikta aktyvi nuoroda yra klaidinga, ir turėjo susilaikyti nuo trečiųjų asmenų nurodymų vykdymo.

Be to, kaip nurodė pareiškėja, ji per „Facebook" tikėjosi parduoti prekę ir už ją į savo sąskaitą gauti pinigines lėšas. Tai reiškia, kad pareiškėja neturėjo tikslo iš savo sąskaitos panaudojant savo mokėjimo priemonės duomenis įvykdyti Operaciją. Tačiau, siekdama už prekę gauti pinigus į savo banko sąskaitą, pareiškėja suvedė personalizuotus saugumo duomenis ir kodų generatoriaus APPLI1 kodą, taip pat tretiesiems asmenims turėjo perduoti kodų generatoriaus APPLI2 kodą. Taigi, tam, kad pareiškėja tariamai į savo banko sąskaitą gautų pinigines lėšas, jos buvo prašoma suvesti personalizuotus duomenis, nors jie įprastai suvedami norint inicijuoti ir patvirtinti mokėjimo operaciją iš banko sąskaitos.

Atkreiptinas dėmesys, kad, norint pinigines lėšas gauti į banko sąskaitą, bankai neprašo sąskaitos turėtojo pateikti savo prisijungimo prie internetinės banko sąskaitos duomenų ir neprašo suvesti kodų generatoriaus APPLI1 kodo arba APPLI2 kodo perduoti lėšų siuntėjui. Taigi, pareiškėja, nors ir turėjo galimybę kritiškai įvertinti savo veiksmų su mokėjimo priemone riziką ir galimas pasekmes, tačiau nuo tolimesnių veiksmų nesusilaikė, o priešingai – vykdė trečiųjų asmenų nurodymus, suvedė savo kodų generatoriaus APPLI1 kodą, be to, APPLI2 kodą turėjo perduoti tretiesiems asmenims, tokiais savo veiksmais pareiškėja leido tretiesiems asmenims patvirtinti Operaciją.

Taigi, šiuo konkrečiu atveju vertinant pareiškėjos elgesį būtent nagrinėjamo ginčo aplinkybių ir prieš pareiškėją nukreiptos specifinės sukčiavimo atakos kontekste, esminėmis aplinkybėmis, vertinant pareiškėjos neatsargumo laipsnį, Lietuvos banko vertinimu, laikytina tai, kad pareiškėjai nesukėlė jokių įtarimų tai, kad jos yra prašoma pateikti visus būtent pačios pareiškėjos prisijungimo prie internetinės banko sąskaitos duomenis, kuriuos ji pripažįsta suvedusi, suvesti kodų generatoriaus APPLI1 kodą, o APPLI2 kodą perduoti tretiesiems asmenims, nors pati pareiškėja tik siekė gauti lėšas, o ne įvykdyti mokėjimo operaciją. Be to, pareiškėjai atsiųsta paslaugų teikėjo „DPD" nuoroda akivaizdžiai skyrėsi nuo teisingos prisijungimo prie tikros bendrovės „DPD" interneto svetainės nuorodos.

Kaip minėta, pagal banko mokėjimo paslaugų teikimo sąlygas, mokėjimo kortelės personalizuotų saugumo duomenų pateikimas minėtose sąlygose numatytais atvejais laikomas kliento (šiuo atveju – pareiškėjos) sutikimu įvykdyti mokėjimo operaciją, lėšas nurašant iš kliento (šiuo atveju – pareiškėjos) sąskaitos. Atitinkamai ginčo byloje nėra jokių duomenų, kad

pareiškėja būtų kvestionavusi paspaudus pranešime atsiųstą nuorodą atsidariusio interneto puslapio autentiškumą ar pačio interneto puslapio neatitikimus, o jei tokių abejonių turėjo, nėra jokių duomenų, kad šias abejones būtų bandžiusi išsklaidyti, patikrinti gautą informaciją.

Papildomai svarbu įvertinti ir tai, kad iš Lietuvos bankui pateiktų duomenų matyti, kad bankas, rūpindamasis klientų saugumu, informavo savo klientus, tarp jų ir pareiškėją, kokios yra saugaus naudojimosi banko teikiamomis el. paslaugomis rekomendacijos. Bankas pateikė duomenis, kad 2022 m. rugpjūčio 25 d. siuntė pareiškėjai pranešimą, kuriuo ragino būti budrią ir niekam neatskleisti duomenų, nespausti jokių nuorodų ir pan. Taigi, iš šių duomenų matyti, kad bankas prevenciškai dėjo pastangas tam, kad pareiškėja būtų supažindinta su sukčiavimo elektroninėje erdvėje rizikomis, taip pat tapatybės patvirtinimo priemonės saugaus naudojimo, jos personalizuotų saugumo žymenų suvedimo ir atskleidimo reikšme bei teisinėmis pasekmėmis.

Išanalizavęs šias bei visas kitas nagrinėjant ginčą nustatytas aplinkybes ir ginčo byloje esančius duomenis, Lietuvos bankas daro išvadą, kad vis dėlto vertinti pareiškėjos elgesio kaip atsargaus ir apdairaus ar tik neatsargaus šiuo atveju nėra galima.

Kaip matyti iš nustatytų aplinkybių, Operaciją tretieji asmenys be pareiškėjos žinios galėjo atlikti tik dėl to, kad pareiškėja, būdamas labai neatsargi, netinkamai įvykdė Mokėjimų įstatyme (34 straipsnis) ir su banku sudarytoje mokėjimo kortelės sutartyje įtvirtintus mokėjimo kortelės saugaus naudojimo reikalavimus. Remiantis nustatytais duomenimis, tam, kad pareiškėja parduotų prekę, jai nebuvo būtina suvesti savo prisijungimo prie internetinės banko paskyros duomenų, kodų generatoriaus APPLI1 kodo arba perduoti tretiesiems asmenims kodų generatoriaus APPLI2 kodo. Tačiau pareiškėja, gavusi trečiųjų asmenų siųstą pranešimą, nedvejodama (kaip pripažįsta pareiškėja) paspaudė jame pateiktą nuorodą ir suklastotame interneto puslapyje nurodė visus trečiųjų asmenų prašomus duomenis, neįsitikinusi nei siųsto pranešimo ir jame pateiktos nuorodos, nei interneto svetainės, į kurią pateko paspaudusi atsiųstą nuorodą, autentiškumu bei prašymo atskleisti konfidencialius savo mokėjimo priemonių duomenis tikrumu.

Nurodytos aplinkybės leidžia teigti, kad pareiškėja būtent dėl savo didelio neatsargumo neišsaugojo personalizuotų saugumo duomenų – nesiėmė tų saugumo priemonių, kurių privalėjo imtis, kad būtų tinkamai apsaugoti jai suteiktos mokėjimo priemonės duomenys, ir taip suteikė tretiesiems asmenims galimybę patvirtinti Operaciją.

Konstatavus, kad pareiškėja, nesilaikydama jai, kaip mokėtojai, Mokėjimų įstatyme ir sutartyje su banku nustatytų pareigų, susijusių su išduotomis mokėjimo priemonėmis, elgėsi labai neatsargiai, kartu darytina išvada, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, nustatančią, kad tokiu atveju mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai. Dėl šios priežasties, Lietuvos banko vertinimu, bankas neturi pareigos grąžinti (kompensuoti) pareiškėjai neautorizuotos Operacijos lėšų.

Įvertinus visa tai, kas išdėstyta pirmiau, ir nustačius, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, darytina išvada, kad pareiškėjos bankui keliamas reikalavimas grąžinti Operacijos sumą – 2 000 Eur, yra nepagrįstas, todėl atmestinas.

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

Atmesti pareiškėjos X. X. reikalavimą.

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