LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

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

2024-06-07 Nr. 429-121
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:

2024 m. sausio 8 d. iš pareiškėjos banko sąskaitos panaudojant tik pareiškėjai žinomus personalizuotus saugos duomenis lėšų gavėjai *Margu Tamm* (toliau – lėšų gavėja) buvo atliktos dvi mokėjimo operacijos, kurių bendra suma 839,64 Eur (toliau – ginčijamos mokėjimo operacijos).

Ginčo byloje nustatyta, kad pareiškėja mobiliuoju telefonu gavo SMS žinutę[1], raginančią paspausti aktyvią nuorodą ir prisijungti neva prie Valstybinės mokesčių inspekcijos (VMI) tikslu perskaityti pranešimą. 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 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 ginčijamas mokėjimo operacijas. Kiekvieną ginčijamą mokėjimo operaciją pareiškėja patvirtino du kartus savo mobiliajame telefone suvesdama tik jai vienai žinomą „Smart-ID" PIN2 kodą.

Remdamasis visa surinkta informacija, bankas priėmė sprendimą atsisakyti pareiškėjai atlyginti jos patirtus nuostolius, nes nustatė, kad ginčijamos mokėjimo operacijos buvo įvykdytos 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 ginčijamų mokėjimo operacijų metu iš jos banko sąskaitos nurašytas lėšas, t. y. grąžinti 839,64 Eur. Pareiškėja Lietuvos bankui paaiškino, kad ji neva iš VMI gavo SMS žinutę, raginančią ją per jai pateiktą aktyvią nuorodą prisijungti prie VMI. Pareiškėja paaiškino, kad dėl tokios SMS žinutės ji nustebusi, nes jokių baudų ji neturėjusi. Pareiškėjos teigimu, kadangi buvo vakaras ir ji buvo labai pavargusi, todėl paspaudė SMS žinutėje jai pateiktą aktyvią nuorodą ir suvedė visus duomenis, reikalingus prisijungti prie savo interneto banko paskyros, įskaitant ir „Smart-ID" paskyros PIN1 kodą. Pareiškėja taip pat teigė, kad prieš patvirtindama ginčijamas mokėjimo operacijas „Smart-ID" paskyros PIN2 kodu ji nematė nei mokėjimo operacijos sumos, nei gavėjo: „pati jokio konkretaus pavedimo nemačiau: nei sumų, nei gavėjo, kitaip tikrai nebūčiau pervedinėjus nežinomam man asmeniui pinigus".

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 ne tik paspaudė jai SMS žinute atsiųstą aktyvią nuorodą, bet ir suvedė savo personalizuotus saugos duomenis, reikalingus prisijungti prie interneto banko paskyros (banko atpažinimo, asmens ir „Smart-ID" PIN1 kodus). Be to, pareiškėja kiekvieną ginčijamą mokėjimo operaciją pati patvirtino suvesdama „Smart-ID" PIN2 kodą, o bankas prieš pareiškėjai suvedant „Smart-ID" PIN2 kodą mobiliojo telefono „Smart-ID" lange

[1] SMS žinutės tekstas: „VMI:gavote nauja pranesima, perskaitykite pranesima prisijungdami cia: https://vmi.roik-73905432950.net."

rodė tiek ginčijamų mokėjimo operacijų sumą, tiek ir lėšų gavėjos 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, vesdama 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 ginčijamas mokėjimo operacijas. Taip pat bankas pažymėjo, kad pareiškėja galėjo suprasti ir įvertinti savo atliekamų veiksmų reikšmę ir pasekmes, nes tokius veiksmus atliko ne pirmą kartą, – „Smart-ID", kaip atpažinimo priemone, pareiškėja naudojasi itin aktyviai, t. y. itin daug kartų jungėsi prie interneto banko, tvirtino mokėjimo operacijas, todėl turėjo nesunkiai suprasti, kad „Smart-ID" PIN2 kodas naudojamas mokėjimo operacijoms tvirtinti.

Be to, bankas pažymėjo, kad „Smart-ID" lange papildomai buvo rodomas keturių skaitmenų kontrolinis kodas, kurį pareiškėja matė „Smart-ID" lange ir turėjo jį sutikrinti su interneto banke rodomu kontroliniu kodu. Banko teigimu, pareiškėjai turėjo kilti įtarimų, kadangi netikrame interneto banko puslapyje kontrolinis kodas nebuvo parodytas.

Bankas pažymėjo, kad iki ginčijamų mokėjimo operacijų įvykdymo bankas pareiškėją buvo informavęs apie sukčiavimo grėsmes naudojantis mokėjimo paslaugomis[2]. Pareiškėjai siųstais pranešimais bankas ją informavo apie saugų naudojimąsi banko nuotoliniais kanalais. Taip pat bankas pažymėjo, kad jis savo interneto svetainėje ir „Facebook" paskyroje skelbia informaciją apie dažniausiai pasitaikančias sukčiavimo atakas ir teikia patarimus banko klientams, kaip išvengti sukčių pinklių.

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 ginčijamų mokėjimo operacijų metu iš jos sąskaitos banke pervestą sumą. Pareiškėja neigia autorizavusi ginčijamas mokėjimo operacijas, todėl mano, kad bankas ginčijamų mokėjimo operacijų lėšas turi jai grąžinti. Banko teigimu, pareiškėjos veiksmams būdingas didelis neatsargumas, todėl bankas negali būti įpareigotas jai grąžinti ginčijamų mokėjimo operacijų 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 nėra jos autorizuotos, 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 ginčijamas mokėjimo operacijas. Dėl šios priežasties yra akivaizdu, kad ginčijamų mokėjimo operacijų 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 ginčijamos mokėjimo operacijos,

[2] 2023 m. balandžio 14 ir 28 d. siuntė SMS žinutes, 2023 m. spalio 30 ir lapkričio 23 d. siuntė pranešimus į pareiškėjos elektroninį paštą.

atliktos nesant pareiškėjos valios ir neišreiškus valinių veiksmų patvirtinti ginčijamas mokėjimo operacijas, laikytinos neautorizuotomis.

Siekdamas išspręsti tarp šalių kilusį ginčą ir įvertinti pareiškėjos bankui keliamo reikalavimo pagrįstumą, Lietuvos bankas vertins, ar bankas, atsisakydamas grąžinti pareiškėjai ginčijamų mokėjimo operacijų metu pervestas lėšas, 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, 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 sąlyga[3].

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 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 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[4]. 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[5].

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[6], 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 tai, kad tai padarė dėl didelio

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

neatsargumo[7].

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 ginčijamų mokėjimo operacijų 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 ginčijamas mokėjimo operacijas, kurias pareiškėja pati patvirtino du kartus suvesdama „Smart-ID" programėlės PIN2 kodą.

Banko sprendimas nekompensuoti pareiškėjos nuostolių dėl neautorizuotų ginčijamų mokėjimo operacijų 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 ginčijamas mokėjimo operacijas, 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 pasitikint SMS žinute gautame pranešime nurodyta informacija ir spaudžiant joje pateiktą nuorodą, suvedant savo mokėjimo priemonės personalizuotus saugumo duomenis suklastotame 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 ginčijamas mokėjimo operacijas.

Lietuvos bankas, įvertinęs pareiškėjos kreipimesi ir banko atsiliepime nurodytas aplinkybes bei kartu su kreipimusi ir atsiliepimu pateiktus duomenis, nustatė, kad prieš ginčijamų mokėjimo operacijų įvykdymą pareiškėja SMS žinute neva iš VMI gavo pranešimą, raginantį ją pasitikrinti VMI paskyroje gautą pranešimą, paspaudė pranešime pateiktą nuorodą ir suklastotame 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 inicijuotos ginčijamos mokėjimo operacijos. Trečiųjų asmenų prisijungimas prie pareiškėjos interneto banko paskyros buvo patvirtintas pačiai pareiškėjai suvedus „Smart-ID" programėlės PIN1 kodą bei vėliau kiekvieną 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 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 mokėtojui[8].

Banko ir pareiškėjos santykiams taip pat taikomas ir banko Paslaugų interneto banke

---

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

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

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 paslaptyje atpažinimo kodą, slaptažodžius, PIN kodus, neužrašyti jų ant generatoriaus ar kitų kartu su juo laikomų daiktų ir jokia kita forma neatskleisti ar nepadaryti jų prieinamų tretiesiems asmenims."

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 paspaudė trečiųjų asmenų atsiųstoje žinutėje esančią aktyvią nuorodą norėdama pasitikrinti neva VMI paskyroje jai pateiktą informaciją, 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 du kartus savo mobiliajame telefone suvedė „Smart-ID" programėlės PIN2 kodą, taip patvirtindama kiekvienos 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 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.

Vis dėlto nagrinėjamo ginčo atveju iš pareiškėjos Lietuvos bankui pateiktos SMS žinutės kopijos matyti, kad pareiškėją telekomunikacijų bendrovė įspėjo, jog SMS žinutė su aktyvia nuoroda https://vmi.roik-7390543290.net yra gauta iš neišsaugoto telefono numerio, taip pat įspėjo pareiškėją saugotis apgaulingų ir apsimestinų žinučių. Atsižvelgiant į pirmiau minėtą informaciją, galima teigti, kad pareiškėjai turėjo kilti įtarimų dėl jai atsiųstos SMS žinutės turinio ir prašomų atlikti veiksmų, juo labiau kad, kaip pati pareiškėja teigė, ji neturėjo jokių baudų VMI. Taigi pareiškėja galėjo susilaikyti nuo tolesnių veiksmų su savo mokėjimo priemone ir imtis veiksmų, kad įsitikintų jai pateiktos nuorodos tikrumu.

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

Be to, ir pats bankas viešai savo „Facebook" paskyroje 2023 m. balandžio 13 d. platino pranešimą[9] ir įspėjo klientus apie sukčių neva iš VMI siunčiamus melagingus pranešimus.

---

[9] https://www.facebook.com/story.php?story_fbid=5960669440716184&id=167427916707061&paipv=0&eav=AfYQwfkcCZ39j-wnLr9nlQU0GP6tAYJHFXCGgKP7r1X5dm6R-W5Eh1D 7aecXZP5vvw&_rdr.

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, VMI svetainėje pasitikrinti informaciją apie gautą baudą. 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 net du kartus suvedė „Smart-ID" programėlės PIN2 kodą, tokiu būdu patvirtindama kiekvienos 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 kiekvienos ginčijamos mokėjimo operacijos įvykdymą bankas pareiškėjai rodė tiek mokėjimo operacijos sumą, tiek ir lėšų gavėjos duomenis – *419,82 EUR i saskaita ***(Duomenys neskelbiami)*. Taigi, pareiškėja, nors ir neturėdama tikslo iš savo banko sąskaitos įvykdyti mokėjimo operacijų, o turėdama tikslą tik prisijungti prie savo interneto banko paskyros, du kartus suvedė „Smart-ID" programėlės PIN2 kodą ir taip patvirtino ginčijamų mokėjimo operacijų 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 ginčijamų mokėjimo operacijų sumą, tiek ir lėšų gavėjos 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 teisines pasekmes, šiuo atveju – mokėjimo priemonės praradimą ir neautorizuotų mokėjimo operacijų iš jos banko sąskaitos įvykdymą.

Įvertinus pirmiau nurodytas aplinkybes, Lietuvos banko nuomone, galima daryti išvadą, kad pareiškėja būtų galėjusi išvengti neautorizuotų mokėjimo operacijų 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 jai atsiųsta SMS žinutė galėjo būti klaidinga, kad jos prašoma atlikti veiksmus, kuriais tvirtinamas mokėjimo operacijų įvykdymas, juolab kad bankas prieš kiekvienos ginčijamos mokėjimo operacijos įvykdymo patvirtinimą rodė tiek mokėjimo operacijos sumą, tiek lėšų gavėjo duomenis. Vis dėlto pareiškėja fakto, kad jos buvo prašoma du kartus suvesti „Smart-ID" PIN2 kodą, nors ji pati ir nesiekė inicijuoti jokių 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 operacijas, kurias pareiškėja pati patvirtino suvesdama „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 įvykdytos neautorizuotos ginčijamos mokėjimo operacijos iš pareiškėjos sąskaitos ir pareiškėja patyrė nuostolių.

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.

Įvertinus pirmiau išdėstytą informaciją, konstatuotina, kad yra pagrindas pareiškėjai taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, todėl pareiškėjos reikalavimas bankui grąžinti neautorizuotų ginčijamų mokėjimo operacijų lėšų sumą yra nepagrįstas ir 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 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