



**LIETUVOS BANKO
TEISĖS IR LICENCIJAVIMO DEPARTAMENTO
DIREKTORIUS**

**SPRENDIMAS
DĖL X.X. IR BANKO LUMINOR BANK AS GINČO NAGRINĖJIMO**

2026-08-20 Nr. 429-299
Vilnius

Lietuvos bankas gavo X.X. (toliau – pareiškėjas) kreipimąsi, kuriuo prašoma išnagrinėti tarp pareiškėjo ir banko *Luminor Bank AS*, veikiančio per skyrių Lietuvoje, (toliau – bankas) kilusį ginčą.

Sprendimo santrauka¹

Ginčas kilo dėl banko pareigos grąžinti (atlyginti) pareiškėjo neautorizuotos mokėjimo operacijos sumą. Mokėjimo operacija buvo inicijuota tretiesiems asmenims neteisėtu būdu pasisavinus pareiškėjo personalizuotus saugos duomenis, prisijungus prie pareiškėjo banko sąskaitos ir inicijavus ginčijamą mokėjimo operaciją, kurios įvykdymą pareiškėjas patvirtino suveddamas „Smart-ID“ PIN2 kodą. Įvertinus šalių pateiktus paaiškinimus ir įrodymus, nustatyta, kad pareiškėjo (mokėtojo) veiksmai su savo mokėjimo priemone pasireiškė dideliu aplaidumu, dėl to bankui nekilo pareiga grąžinti (atlyginti) neautorizuotos mokėjimo operacijos sumos, todėl nėra pagrindo tenkinti pareiškėjo reikalavimo.

N u s t a t y t a:

Esminės faktinės kilusio ginčo aplinkybės

2025 m. gegužės 10 d. iš pareiškėjo banko sąskaitos buvo atlikta 2 999 Eur mokėjimo operacija (toliau – ginčijama mokėjimo operacija) lėšų gavėjai X.X. (toliau – lėšų gavėjas).

Iš ginčo byloje pateiktų duomenų matyti, kad 2025 m. gegužės 10 d. pareiškėjas siekė prisijungti prie Valstybinės mokesčių inspekcijos prie Lietuvos Respublikos finansų ministerijos (toliau – VMI) elektroninio deklaravimo sistemos (toliau – EDS). Pareiškėjas, siekdamas patekti į EDS ir (arba) VMI interneto svetainę, pasinaudojo interneto paieškos sistema „Google“, jos paieškos laukelyje įvedė su VMI susijusį raktažodį ir iš pateiktų paieškos rezultatų pasirinko nuorodą, nukreipusią jį į trečiųjų asmenų sukurtą suklastotą interneto svetainę.

Suklastotoje interneto svetainėje pareiškėjui buvo nurodyta patvirtinti savo tapatybę prisijungiant per interneto banką. Pareiškėjas suvedė jam asmeniškai suteiktą individualų prisijungimo prie interneto banko kodą, o savo tapatybę papildomai patvirtino „Smart-ID“ PIN1 kodu. Pareiškėjui suvedus minėtus personalizuotus saugumo duomenis, tretiesiems asmenims buvo sudaryta galimybė pareiškėjo vardu prisijungti prie jo interneto banko paskyros ir inicijuoti ginčijamą mokėjimo operaciją, ją pareiškėjas patvirtino suveddamas „Smart-ID“ PIN2 kodą.

Remdamasis visa surinkta informacija, bankas priėmė sprendimą atsisakyti pareiškėjui atlyginti jo patirtus nuostolius, nes nustatė, kad ginčijama mokėjimo operacija buvo įvykdyta panaudojus tik pareiškėjui žinomus personalizuotus saugos duomenis bei pačiam pareiškėjui suvedus savo „Smart-ID“ PIN1 ir PIN2 kodus. Banko vertinimu, pareiškėjas dėl savo didelio neatsargumo atskleidė savo mokėjimo priemonės duomenis tretiesiems asmenims, todėl patyrė nuostolių. Pareiškėjas su tuo nesutiko, todėl tarp šalių kilo ginčas.

Ginčo reikalavimai

Įpareigoti banką atlyginti nuostolius, patirtus dėl neautorizuotos mokėjimo operacijos

¹ Santraukoje pateikiami tik trumpi nagrinėto vartojimo ginčo apibendrinimai. Norint suprasti ir (ar) įvertinti sprendime aptariamas aplinkybes, sprendimo dėl šio ginčo esmės pagrindus ir motyvus, būtina tinkamai susipažinti su viso sprendimo turiniu.

įvykdymo – 2 999 Eur.

Ginčo šalių pateikti paaiškinimai

Pareiškėjas Lietuvos bankui paaiškino, kad jis ginčijamos mokėjimo operacijos neautorizavo, o bankas prieš jam vedant „Smart-ID“ PIN2 kodą nerodė ginčijamos mokėjimo operacijos sumos. Pateikdamas papildomus paaiškinimus, pareiškėjas teigė, kad tvirtindamas ginčijamą mokėjimo operaciją siekė atlikti 45,48 Eur mokėjimą VMI. Pareiškėjas paaiškino, kad mokėjimo procesą pradėjo VMI interneto svetainėje, kurioje jam buvo nurodyta konkreti mokėtina 45,48 Eur suma. VMI sistemoje pasirinkęs galimybę atlikti mokėjimą per banką, pareiškėjas buvo automatiškai nukreiptas į, jo supratimu, banko mokėjimo langą, skirtą šiam konkrečiam mokėjimui atlikti. Pareiškėjas teigia pats interneto banke nevedęs nei mokėjimo gavėjo duomenų, nei sąskaitos numerio, nei kitų mokėjimo rekvizitų.

Pareiškėjo teigimu, kadangi šį mokėjimą jis inicijavo pats, „Smart-ID“ programėlėje pateiktą prašymą įvesti PIN2 kodą ir rodomą kontrolinį kodą jis suprato kaip jo paties inicijuoto 45,48 Eur mokėjimo VMI patvirtinimą. Pareiškėjas pažymėjo neturėjęs techninės galimybės tapatybės patvirtinimo priemonės ekrane matyti, kad tretieji asmenys galėjo pakeisti mokėjimo gavėją ir mokėjimo sumą, todėl manė tvirtinantis savo inicijuotą mokėjimą VMI.

Atsižvelgdamas į nurodytas aplinkybes, pareiškėjas mano, kad tapo sudėtingos sukčiavimo atakos auka ir, įvesdamas „Smart-ID“ PIN2 kodą, neturėjo tikslo patvirtinti ginčijamos mokėjimo operacijos.

Atsiliepime į pareiškėjo kreipimąsi bankas nurodo nesutinkąs su pareiškėjo reikalavimu ir prašo jį atmesti. Bankas paaiškino, kad pareiškėjas dėl didelio neatsargumo neišsaugojo savo personalizuotų saugos duomenų, todėl tretieji asmenys jais galėjo pasinaudoti ir be pareiškėjo žinios inicijuoti ginčijamą mokėjimo operaciją. Banko teigimu, pareiškėjo didelis neatsargumas pasireiškė tuo, kad pareiškėjas nekrepė dėmesio į banko prieš ginčijamos mokėjimo operacijos patvirtinimą rodomą informaciją, nors bankas, prieš pareiškėjui vedant „Smart-ID“ PIN2 kodą, rodė informaciją apie ginčijamos mokėjimo operacijos sumą bei gavėjo duomenis.

Pateikdamas papildomus paaiškinimus bankas nurodo, kad pareiškėjo teiginys, jog jis ketino sumokėti 45 Eur baudą, todėl „Smart-ID“ PIN2 kodo įvedimas jam atrodė logiškas ir pagrįstas, neatitinka banko nustatytų faktinių aplinkybių. Banko teigimu, norėdamas sumokėti baudą, pareiškėjas visų pirma turėjo sėkmingai prisijungti prie VMI sistemos, joje susipažinti su informacija apie mokėtiną baudą ir atlikti papildomus veiksmus, būtinus mokėjimui inicijuoti. Tik atlikęs šiuos veiksmus Pareiškėjas galėjo būti nukreiptas į mokėjimo per banką inicijavimo ir patvirtinimo procesą. Banko vertinimu, pareiškėjas nepateikė jokių objektyvių duomenų, patvirtinančių, kad jam buvo pavykę prisijungti prie VMI sistemos, joje buvo pateikta informacija apie mokėtiną 45 Eur baudą ar kad pareiškėjas šioje sistemoje buvo inicijavęs tokios baudos apmokėjimą. Atsižvelgdamas į tai, bankas mano, kad pareiškėjas neturėjo pagrindo „Smart-ID“ programėlėje pateikto prašymo įvesti PIN2 kodą siesti su jo nurodomu mokėjimu VMI.

Bankas teigia ir tai, kad, rūpindamasis lėšų saugumu, periodiškai informuoja savo klientus, įskaitant ir pareiškėją, apie dažniausiai pasitaikančias sukčiavimo atakas bei primena, kokios yra saugaus naudojimosi banko teikiamomis el. paslaugomis rekomendacijos.

Atsižvelgdamas į visas pirmiau nurodytas aplinkybes, bankas prašė atmesti pareiškėjo 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. Lietuvos bankas ginčo nagrinėjimo proceso metu neatlieka Lietuvos Respublikos Lietuvos banko įstatymo 42¹ straipsnyje reglamentuotų patikrinimų, skirtų faktinėms aplinkybėms, susijusioms su Lietuvos banko prižiūrimo finansų rinkos dalyvio galimu Lietuvos banko kompetencijai priskirtų teisės aktų reikalavimų pažeidimu, nustatyti ir įvertinti. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Teisinis vertinimas

Pareiškėjo ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjui ginčijamos mokėjimo operacijos metu iš jo sąskaitos banke pervestą sumą. Pareiškėjas neigia autorizavęs ginčijamą mokėjimo operaciją ir teigia, kad bankas neprašė suvesti „Smart-ID“ PIN2 kodo. Banko teigimu, pareiškėjo veiksams būdingas didelis neatsargumas, todėl bankas negali būti įpareigotas 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).

Pareiškėjo nurodytos aplinkybės, kad ginčijama mokėjimo operacija nėra jo autorizuota, o pareiškėjo personalizuotus saugumo duomenis tretieji asmenys gavo apgaulės būdu, bankas atsiliepime neginčija. Priešingai, bankas savo paaiškinimuose nurodo, kad dėl pareiškėjo atskleistų duomenų tretieji asmenys įgijo galimybę inicijuoti ginčijamą mokėjimo operaciją. Dėl šios priežasties yra akivaizdu, kad ginčijamos mokėjimo operacijos inicijavimas ir patvirtinimas neatitiko paties pareiškėjo valios, nors formaliai (pagal išorinius požymius) ir sutapo su pareiškėjo ir banko sutarta sutikimo atlikti mokėjimo operaciją davimo forma ir tvarka. Atsižvelgdamas į tai, Lietuvos bankas daro išvadą, kad ginčijama mokėjimo operacija, atlikta nesant pareiškėjo valios ir neišreiškus valinių veiksmų patvirtinti ginčijamą mokėjimo operaciją, laikytina neautorizuota.

*Siekiant išspręsti tarp pareiškėjo ir banko kilusį ginčą, Lietuvos banko vertinimu, būtina nustatyti, ar bankas **turi pareigą grąžinti pareiškėjui įvykdytos ginčijamos mokėjimo operacijos sumą.***

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. Todėl tuo atveju, jei mokėtojas elgiasi nesąžiningai ar 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 pareiškėjas 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 pareiškėjui ginčijamos mokėjimo operacijos sumą laikytinas pagrįstu, būtina įvertinti, ar pareiškėjo elgesys, atskleidžiant tretiesiems asmenims personalizuotus saugumo duomenis, vertintinas kaip didelis

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

neatsargumas, dėl kurio su mokėjimo operacijos įvykdymu atsiradę nuostoliai, kaip nustatyta Mokėjimų įstatymo 39 straipsnio 3 dalyje, tektų pačiam pareiškėjui.

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 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 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).

Banko sprendimas nekompensuoti pareiškėjo nuostolių dėl neautorizuotos ginčijamos mokėjimo operacijos įvykdymo galėtų būti vertinamas kaip pagrįstas tik tuo atveju, jeigu būtų įrodyta, kad pareiškėjas, suveddamas ir panaudodamas savo mokėjimo priemonės personalizuotus saugumo duomenis, sudarė tretiesiems asmenims galimybę inicijuoti ginčijamą mokėjimo operaciją ir pats ją patvirtino, elgdamasis itin aplaidžiai, t. y. labai neatsargiai.

Bankas mano, kad nuostolius dėl ginčijamos mokėjimo operacijos pareiškėjas patyrė dėl savo didelio neatsargumo, t. y. atskleidždamas tretiesiems asmenims savo banko atpažinimo kodą bei suveddamas tik jam žinomus „Smart-ID“ PIN1 ir PIN2 kodus ir taip suteikdamas leidimą pareiškėjo vardu tretiesiems asmenims ne tik prisijungti prie pareiškėjo interneto banko, inicijuoti ginčijamą mokėjimo operaciją, bet ir pačiam pareiškėjui patvirtinant jos įvykdymą.

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

Lietuvos bankas, siekdamas nustatyti, ar pareiškėjo elgesys šiuo atveju gali būti laikomas labai neatsargiu, vertino pareiškėjo veiksmus, atliktus siekiant prisijungti prie VMI, jo veiksmus paspaudžiant interneto paieškos sistemoje pateiktą nuorodą, suvedant savo personalizuotus saugumo duomenis suklustotoje interneto svetainėje ir patvirtinant atliekamus veiksmus „Smart-ID“ PIN1 bei PIN2 kodais. Taip pat buvo vertinami banko pateikti duomenys apie ginčijamos mokėjimo operacijos inicijavimą ir patvirtinimą bei banko veiksmai, kurių jis ėmėsi tam, kad supažindintų pareiškėją su elektroninėje erdvėje kylančiomis sukčiavimo rizikomis ir saugaus tapatybės patvirtinimo priemonės naudojimo reikalavimais.

Lietuvos bankas, įvertinęs pareiškėjo kreipimesi ir banko atsiliepime nurodytas aplinkybes bei kartu su kreipimusi ir atsiliepimu pateiktus duomenis, nustatė, kad 2025 m. gegužės 10 d. pareiškėjas siekė prisijungti prie VMI. Banko vertinimu, tikėtina, kad pareiškėjas pasinaudojo interneto paieškos sistema „Google“, jos paieškos laukelyje įvedė su VMI susijusį

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 bylos Nr. [2022-02496](#).

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

raktažodį ir iš pateiktų paieškos rezultatų pasirinko nuorodą, nukreipusią jį į trečiųjų asmenų sukurtą suklastotą interneto svetainę.

Pareiškėjas neneigia, kad šioje interneto svetainėje suvedė savo individualų prisijungimo prie interneto banko kodą ir „Smart-ID“ PIN1 kodu patvirtino savo tapatybę. Šiais veiksmais tretiesiems asmenims buvo sudaryta galimybė pareiškėjo vardu prisijungti prie jo interneto banko paskyros. Prisijungę prie pareiškėjo interneto banko paskyros, tretieji asmenys suformavo 2 999 Eur momentinio mokėjimo nurodymą lėšų gavėjui.

Pareiškėjas paaiškino, kad tvirtindamas ginčijamą mokėjimo operaciją siekė atlikti ne 2 999 Eur mokėjimą lėšų gavėjui, o 45,48 Eur mokėjimą VMI. Pareiškėjo teigimu, jo naudojamoje interneto svetainėje buvo nurodyta būtent 45,48 Eur mokėtina suma, kai pasirinko mokėjimą per banką „Luminor“, jis buvo automatiškai nukreiptas į, jo supratimu, banko mokėjimo integracijos langą. Pareiškėjas taip pat nurodė, kad pats interneto banke nevedė gavėjo sąskaitos numerio, mokėjimo sumos ar kitų mokėjimo rekvizitų, todėl „Smart-ID“ programėlėje pateiktą prašymą įvesti PIN2 kodą suprato kaip jo paties inicijuoto 45,48 Eur mokėjimo VMI patvirtinimą.

Bankas su tokiais pareiškėjo argumentais nesutinka ir nurodo, kad pareiškėjas nepateikė jokių objektyvių duomenų, patvirtinančių, jog jam buvo pavykę sėkmingai prisijungti prie tikrosios VMI sistemos, joje susipažinti su informacija apie mokėtiną 45,48 Eur sumą ar inicijuoti šios sumos sumokėjimą. Banko teigimu, siekdamas atlikti mokėjimą VMI, pareiškėjas pirmiausia būtų turėjęs prisijungti prie tikrosios VMI sistemos, joje atlikti mokėjimui inicijuoti būtinus veiksmus ir tik tada būti nukreiptas į mokėjimo per banką patvirtinimo procesą.

Kaip jau buvo minėta pirmiau, 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.

Banko ir pareiškėjo santykius reglamentuojančių banko Mokėjimo paslaugų teikimo taisyklių (toliau – Taisyklės) 7.3.4 papunktyje reglamentuojama, kad klientas privalo užtikrinti jam patikėtų atpažinimo priemonių saugumą: „neturi teisės jų perduoti nei kitam asmeniui, nei kitam Sąskaitos valdytojui, nei bet kokiam kitam Kliento atstovui; įsipareigoja laikyti juos paslapyje, nerašyti jų ant popieriaus, ant kitokių daiktų bei laikyti kitokiame, išskyrus Banko suteiktame, pavidale“.

Taisyklių 9.1 papunktyje nustatyta, kad klientas naudodamasis jam išduota mokėjimo priemone turi pareigą naudotis mokėjimo priemone pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, gavęs mokėjimo priemonę, imtis veiksmų, kad apsaugotų personalizuotus saugumo duomenis.

Taigi, pirmiau aptartos Taisyklių nuostatos aiškiai nustato, kad už tapatybės patvirtinimo priemonės personalizuotų saugumo duomenų konfidencialumo išsaugojimą yra atsakingas mokėtojas, šiuo atveju – pareiškėjas.

Atsižvelgiant į tai, manytina, kad pareiškėjo elgesys būtų laikomas atitinkančiu mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, jeigu būtų nustatyta, kad pareiškėjas ėmėsi pakankamų veiksmų arba, priešingai, susilaikė nuo tam tikrų veiksmų tam, kad banko jam išduotos mokėjimo priemonės personalizuotų saugumo duomenų, suteikiančių galimybę prisijungti prie interneto banko, inicijuoti ir patvirtinti mokėjimus, konfidencialumas būtų tinkamai užtikrintas, o banko išduota mokėjimo priemonė būtų naudojama šalių sutartinius santykius reglamentuojančiuose dokumentuose nustatyta tvarka ir sąlygomis.

Pažymėtina, kad sukčiavimo atakos, kurių metu naudojamos suklastotos valstybės institucijų ar finansų įstaigų interneto svetainės ir siekiama išgauti mokėjimo paslaugų vartotojų prisijungimo bei tapatybės patvirtinimo duomenis, nėra naujos. Apie tokias sukčiavimo atakas periodiškai skelbiama viešai, o vartotojai raginami kritiškai vertinti interneto paieškos sistemose pateikiamas nuorodas ir prieš suvesdami personalizuotus saugumo duomenis įsitikinti, kad naudojasi tikra paslaugų teikėjo interneto svetaine.

Atsižvelgiant į pirmiau minėtą informaciją, galima teigti, kad pareiškėjui galėjo kilti įtarimų dėl interneto svetainės, į kurią jis pateko, tikrumo. Pareiškėjas, jeigu būtų neskubėjęs vykdyti interneto svetainėje pateiktų nurodymų ir kritiškai įvertinęs prašymą suvesti prisijungimo prie interneto banko duomenis, būtų galėjęs suprasti arba bent įtarti, kad prieš jį gali būti vykdoma sukčiavimo ataka.

Vertinant, ar pareiškėjo elgesys, kai jis, siekdamas prisijungti prie VMI sistemos ir atlikti,

jo teigimu, 45,48 Eur mokėjimą VMI, paspaudė interneto paieškos sistemoje pateiktą nuorodą, suklasztotoje interneto svetainėje suvedė savo individualų prisijungimo prie interneto banko kodą ir „Smart-ID“ PIN1 kodą, taip sudarydamas tretiesiems asmenims galimybę jo vardu prisijungti prie interneto banko ir inicijuoti ginčijamą mokėjimo operaciją, o vėliau jos įvykdymą patvirtino „Smart-ID“ PIN2 kodu, gali būti vertinamas kaip labai neatsargus, svarbu įvertinti visų pareiškėjo atliktų veiksmų visumą.

Vertinant pareiškėjo veiksmus su jam išduotos mokėjimo priemonės personalizuotais saugumo duomenimis, svarbu tai, kad pareiškėjas neturėjo tikslo iš savo banko sąskaitos įvykdyti 2 999 Eur mokėjimo operacijos lėšų gavėjui, jis teigia siekęs atlikti 45,48 Eur mokėjimą VMI. Būtent siekdamas atlikti šį mokėjimą pareiškėjas suvedė savo personalizuotus saugumo duomenis ir panaudojo „Smart-ID“ PIN1 bei PIN2 kodus.

Vis dėlto ginčo byloje nėra objektyvių duomenų, patvirtinančių, kad prieš įvesdamas „Smart-ID“ PIN2 kodą pareiškėjas buvo sėkmingai prisijungęs prie tikrosios VMI sistemos, joje buvo suformuotas 45,48 Eur mokėjimas ir buvo pradėtas šio mokėjimo inicijavimo procesas. Priešingai, iš banko pateiktų duomenų matyti, kad, tretiesiems asmenims gavus prieigą prie pareiškėjo interneto banko paskyros, buvo suformuotas 2 999 Eur momentinio mokėjimo nurodymas lėšų gavėjui, jo vykdymas buvo patvirtintas pareiškėjo naudojama „Smart-ID“ tapatybės patvirtinimo priemone ir PIN2 kodu.

Ginčo byloje nėra duomenų, kad pareiškėjo mobilusis įrenginys ar jame įdiegta „Smart-ID“ programėlė ginčijamos mokėjimo operacijos patvirtinimo metu būtų buvę ne pareiškėjo žinioje. Pareiškėjas taip pat neneigia, kad pats įvedė „Smart-ID“ PIN2 kodą, tačiau teigia manęs, kad šiuo kodu tvirtina savo inicijuotą 45,48 Eur mokėjimą VMI.

Remiantis banko Lietuvos bankui pateiktu išrašu iš banko vidinių sistemų dėl ginčijamos mokėjimo operacijos, bankas prieš pareiškėjui suvedant „Smart-ID“ PIN2 kodą rodė tokią informaciją: „confirmationMessage“, „displayText200“: „Luminor Bank AS. Patvirtinti mokejima 2999.00 EUR ***4209 X.X.“

Taigi, pareiškėjas, nors ir turėjo galimybę kritiškai įvertinti savo veiksmų su mokėjimo priemone riziką ir galimas pasekmes ir turėjo galimybę susilaikyti nuo tolimesnių veiksmų, tačiau nuo jų nesusilaikė, priešingai, vykdė trečiųjų asmenų nurodymus ir suvedė savo „Smart-ID“ PIN1 ir PIN2 kodus.

Įvertinus pirmiau nurodytas aplinkybes, Lietuvos banko nuomone, galima daryti išvadą, kad, jeigu pareiškėjas būtų buvęs pakankamai kritiškas savo su mokėjimo priemone atliekamų veiksmų atžvilgiu ir būtų susilaikęs nuo veiksmų su savo mokėjimo priemone, jis būtų galėjęs išvengti neautorizuotos mokėjimo operacijos iš savo sąskaitos įvykdymo. Pareiškėjas turėjo galimybę suprasti, kad jo prašoma patvirtinti 2 999 Eur mokėjimo operaciją, ir turėjo kritiškai įvertinti trečiųjų asmenų prašomus atlikti veiksmus su savo mokėjimo priemone.

Vis dėlto pareiškėjas nekreipė tinkamo dėmesio į banko jam pateiktą informaciją, vykdė trečiųjų asmenų jam pateiktus nurodymus. Lietuvos banko vertinimu, toks pareiškėjo elgesys gali būti pripažintas kaip elgesys, iš esmės besiskiriantis nuo atsargaus elgesio reikalavimų, tai galiausiai ir lėmė, kad pareiškėjas prarado savo mokėjimo priemonę, o tretieji asmenys įgijo galimybę pareiškėjo vardu inicijuoti ginčijamą mokėjimo operaciją.

Taigi, įvertinus ginčo byloje turimus duomenis bei ginčo šalių paaiškinimus apie mokėjimo operacijos įvykdymo aplinkybes, galima teigti, kad pareiškėjas mokėjimo priemone naudojosi nesilaikydamas 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 pareiškėjo veiksmai, dėl kurių jis prarado mokėjimo priemonę, pasireiškė dideliu neatsargumu, tai galiausiai ir lėmė, kad buvo įvykdyta neautorizuota ginčijama mokėjimo operacija iš pareiškėjo sąskaitos ir pareiškėjas patyrė nuostolių. Mokėjimų įstatymo 39 straipsnio 3 dalyje nustatyta, kad mokėtojai tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai, jeigu jis juos patyrė veikdamas nesažiningai arba tyčia ar dėl didelio neatsargumo neįvykdęs vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų.

Įvertinus pirmiau išdėstytą informaciją, konstatuotina, kad yra pagrindas pareiškėjui taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį.

Išvada

Nenustačius pagrindo tenkinti pareiškėjo reikalavimo bankui dėl ginčijamos mokėjimo operacijos sumos grąžinimo (atlyginimo), pareiškėjo reikalavimas 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 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 pareiškėjo 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.