



**LIETUVOS BANKO
TEISĖS IR LICENCIJAVIMO DEPARTAMENTO
DIREKTORIUS**

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

2023-07-19 Nr. 429-422
Vilnius

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

N u s t a t y t a:

2023 m. balandžio 19 d. iš pareiškėjo sąskaitos banke pareiškėjui banko išduota mokėjimo kortele buvo inicijuota 2 000 Eur mokėjimo operacija (toliau – mokėjimo operacija) gavėjui CTX (toliau – gavėjas). Mokėjimo operacija buvo įvykdyta po to, kai pareiškėjas vykdydamas trečiųjų asmenų nurodymus paspaudė jam elektroniniu paštu atsiųstą neva Valstybinės mokesčių inspekcijos (toliau – VMI) aktyvią nuorodą ir atidarytame neva interneto banko puslapyje, tikėdamasis į savo banko sąskaitą gauti sumokėtų mokesčių permoką, suvedė savo banko naudotojo ID, asmens kodą, mokėjimo kortelės duomenis, šiuos duomenis nusavino tretieji asmenys ir inicijavo prisijungimą prie pareiškėjo naudojamos banko išmaniosios programėlės iš kito (pareiškėjui nepriklausančio) mobiliojo telefono įrenginio. Suveddamas savo „Smart-ID“ PIN1 kodą, pareiškėjas patvirtino trečiųjų asmenų prisijungimą pareiškėjo vardu prie pareiškėjo banko išmaniosios programėlės. Tretieji asmenys pasinaudoję iš pareiškėjo nusavintais personalizuotais saugos duomenimis inicijavo mokėjimo operaciją ir ją patvirtino savo mobiliojo telefono įrenginyje įdiegtais biometriniais duomenimis.

Bankui atsisakius pareiškėjui gražinti mokėjimo operacijos sumą, pareiškėjas kreipėsi į Lietuvos banką prašydamas išnagrinėti vartojimo ginčą ir gražinti bent dalį neautorizuotos mokėjimo operacijos sumos. Pareiškėjas paaiškino, kad elektroniniu paštu neva iš VMI gavo laišką, kuriuo buvo informuotas apie jam VMI gražintinas lėšas ir šiuo tikslu jo buvo prašoma paspausti aktyvią nuorodą. Pareiškėjas teigia paspaudęs šią aktyvią nuorodą ir suvedęs jo prašomus duomenis, tikėdamasis, kad jungiasi prie savo banko sąskaitos. Tačiau netrukus po to pareiškėjas iš banko gavo SMS žinutę, kad iš jo banko sąskaitos buvo nurašyta 2 000 Eur suma, tada suprato, kad tapo sukčių auka. Pareiškėjas teigia iš karto kreipėsis į banką, o mokėjimo operacijos lėšos jo banko sąskaitoje buvo dar tik rezervuotos, todėl bankas turėjo galimybę atšaukti mokėjimo operaciją ir sugražinti jam lėšas. Pareiškėjas pripažįsta, kad jam reikėjo būti atsargesniam, tačiau pabrėžia, kad yra kurčnebylis ir nebuvo daug girdėjęs apie sukčiavimo atvejus. Pareiškėjas prašė nustatyti, ar banko darbuotojai neatšaukdami mokėjimo operacijos padarė viską, ką galėjo, ir bent iš dalies kompensuoti pareiškėjo dėl neautorizuotos mokėjimo operacijos patirtus nuostolius.

Bankas Lietuvos bankui pateiktame atsiliepime paaiškino, kad pareiškėjas dėl didelio neatsargumo neišsaugojo savo personalizuotų saugos duomenų, todėl tretieji asmenys jais galėjo pasinaudoti ir be pareiškėjo žinios inicijuoti mokėjimo operaciją. Banko teigimu, pareiškėjo didelis neatsargumas pasireiškė tuo, kad pareiškėjas, gavęs neva iš VMI elektroninį laišką su aktyvia nuoroda ir ją paspaudęs patekęs į neva banko interneto puslapį, nesutikrino jam pateikto interneto banko adresu su tikruoju banko interneto banko adresu, nors bankas savo interneto puslapyje pateikia informaciją, kaip patikrinti, ar interneto banko svetainės adresas yra teisingas. Bankas taip pat pažymėjo, kad pareiškėjas savo mokėjimo priemone naudojo ne pagal paskirtį: norinčių prisijungti prie savo interneto banko paskyros nėra prašoma suvesti mokėjimo kortelės duomenų, priešingai – mokėjimo kortelės duomenys yra naudojami tam, kad būtų inicijuota mokėjimo operacija. Bankas taip pat teigė, kad, prieš pareiškėjui suvedant savo „Smart-ID“ PIN1 kodą, bankas jam rodė informaciją, kokiu tikslu pareiškėjo

prašoma suvesti „Smart-ID“ PIN1 kodą: „Patvirtinkite informaciją Norėdami tęsti, įsitikinkite, kad jūsų operacijos informacija yra teisinga Approve this device iPhone (iPhone 13 Pro Max) for app login „Patvirtinti“ „Atšaukti“. Bankas informavo, kad pareiškėjas naudojo mobilųjį telefono įrenginį *Xiaomi 22021211RG*, o trečiųjų asmenų naudojamas mobiliojo telefono įrenginys – *iPhone 13 Pro Max*, jo pavadinimas netgi vizualiai nebuvo panašus į pareiškėjo naudojamą įrenginį, todėl pareiškėjas nesunkiai galėjo pastebėti šį skirtumą.

Bankas paaiškino, kad savo klientus, tarp jų ir pareiškėją, periodiškai informuoja apie vykstančias sukčiavimo atakas tiek interneto banko žinutėmis, tiek išmaniojoje programėlėje, tiek ir banko interneto puslapyje. Apie vykstančias naujas sukčiavimo atakas, prisidengiant VMI vardu, banko teigimu, buvo plačiai informuota visuomenė tiek pačios VMI, tiek Lietuvos banko, tiek policijos, tiek žiniasklaidos įvairiais kanalais ir būdais. Todėl, banko teigimu, nėra pagrįsti pareiškėjo argumentai, kad jis dėl klausos negalios negalėjo susipažinti su informacija apie sukčiavimo atakas, nes informacija buvo teikiama ir raštu.

Pasisakydamas dėl pareiškėjo argumento, kad bankas turėjo galimybę atšaukti mokėjimo operaciją, tačiau jos neatsaukė, bankas pabrėžė, kad šis pareiškėjo argumentas yra esminis, juo pareiškėjas grindžia savo reikalavimą bankui bent iš dalies kompensuoti nuostolius dėl mokėjimo operacijos įvykdymo. Bankas paaiškino, kad galimybių atšaukti banko ir pareiškėjo sutartu būdu patvirtintos mokėjimo operacijos po to, kai bankas gavo mokėjimo nurodymą, nebuvo. Kad mokėjimo operacija būtų atšaukta, būtinas lėšų gavėjo sutikimas, taigi, bankas savo iniciatyva negali atšaukti mokėjimo operacijos ir iš pareiškėjo banko sąskaitos panaikinti lėšų rezervacijos.

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 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 pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Pareiškėjo ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjui pareiškėjo vardu banke atidarytoje sąskaitoje kortele atliktos mokėjimo operacijos lėšas, iš viso 2 000 Eur. Pareiškėjas teigia nenorėjęs įvykdyti mokėjimo operacijos, tačiau ir neneigia paspaudęs trečiųjų asmenų jam atsiųstą neva VMI nuorodą ir trečiųjų asmenų suklastotame banko interneto puslapyje pats suvedęs savo banko atpažinimo ID, asmens kodą, mokėjimo kortelės duomenis, suvedęs savo „Smart-ID“ PIN1 kodą ir taip patvirtinęs trečiųjų asmenų prisijungimą prie pareiškėjo išmaniosios programėlės iš kito pareiškėjui nepriklausančio mobiliojo telefono įrenginio, tai ir lėmė mokėjimo operacijos iš jo sąskaitos įvykdymą.

Pareiškėjo teigimu, tuo metu, kai jis kreipėsi į banką ir prašė atšaukti mokėjimo operaciją, mokėjimo operacijos lėšos pareiškėjo sąskaitoje buvo dar tik rezervuotos, todėl bankas galėjo atšaukti mokėjimo operacijos vykdymą ir grąžinti pareiškėjui mokėjimo operacijos lėšas. Bankas teigia, kad pareiškėjo mokėjimo operacija buvo patvirtinta šalių sutarta forma ir tvarka, dėl to bankas ją pagrįstai įvykdė, o pareiškėjas į banką dėl mokėjimo operacijos atšaukimo kreipėsi po to, kai mokėjimo nurodymas buvo gautas banke, todėl bankas mokėjimo operacijos be gavėjo sutikimo atšaukti negalėjo. Taip pat bankas teigia, kad yra sąlygos pareiškėjo elgesį, prarandant savo mokėjimo priemonę, vertinti kaip labai neatsargų, todėl bankas mano, kad neturi pareigos kompensuoti pareiškėjui jo patirtų nuostolių dėl įvykdytos mokėjimo operacijos. Dėl šių priežasčių, banko nuomone, visi mokėjimo operacijos nuostoliai turėtų tekti pareiškėjui.

Svarbu pažymėti, kad tarp šalių nėra ginčo, kad nebuvo duotas pareiškėjo sutikimas vykdyti mokėjimo operaciją, t. y. tiek pareiškėjas, tiek bankas pripažįsta, kad mokėjimo operaciją inicijavo ne pats pareiškėjas, o tretieji asmenys, neteisėtu būdu pasisavinę pareiškėjo mokėjimo priemonę. Atsiliepiame bankas iš esmės remiasi Lietuvos Respublikos mokėjimų įstatymo nuostatomis, reglamentuojančiomis mokėtojo atsakomybę už neautorizuotas mokėjimo operacijas. Taigi, galima daryti išvadą, kad bankas pripažįsta, kad mokėjimo operacija nagrinėjamo ginčo atveju laikytina neautorizuota. Atsižvelgiant į tai, kad iš esmės abi

ginčo šalys sutaria, kad mokėjimo operacija galėjo būti inicijuota be pareiškėjo žinios ir sutikimo, toliau sprendime nebus analizuojamos su mokėjimo operacijos autorizavimo vertinimu susijusios aplinkybės, o mokėjimo operacija laikoma pareiškėjo neautorizuota.

Siekdamas išspręsti tarp šalių kilusį ginčą ir įvertinti pareiškėjo bankui keliamo reikalavimo pagrįstumą, Lietuvos bankas vertins, ar: 1) bankas turi pareigą grąžinti ir (ar) kompensuoti pareiškėjui mokėjimo operacijos sumą; 2) bankas turėjo pareigą atšaukti mokėjimo operaciją.

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 Mokėjimų įstatymas.

1. Dėl neautorizuotos mokėjimo operacijos pasekmių ir pareiškėjo teisės į mokėjimo operacijos sumos grąžinimą

Pagal Mokėjimų įstatymo 39 straipsnio 1 dalį, mokėtojai gali tekti dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai iki 50 eurų, kai šie nuostoliai patirti dėl: 1) prarastos ar pavogtos mokėjimo priemonės panaudojimo; 2) neteisėto mokėjimo priemonės pasisavinimo. Tačiau, kaip nustatyta Mokėjimų įstatymo 39 straipsnio 2 dalyje, mokėtojas neturi patirti jokių nuostolių, jeigu jis iki mokėjimo operacijos įvykdymo negalėjo pastebėti mokėjimo priemonės praradimo, vagystės arba neteisėto pasisavinimo, išskyrus atvejus, kai jis veikė nesažiningai (1 punktas).

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 neįvykdyęs vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų. Tokiais atvejais Mokėjimų įstatymo 39 straipsnio 1 dalyje nustatytas didžiausias nuostolių sumos ribojimas netaikomas.

Pagal Mokėjimų įstatymo 2 straipsnio 32 dalį, mokėjimo priemonė – personalizuota priemonė ir (arba) tam tikros procedūros, dėl kurių susitaria mokėjimo paslaugų vartotojas ir mokėjimo paslaugų teikėjas ir kurias mokėjimo paslaugų vartotojas naudoja mokėjimo nurodymui inicijuoti. Pasisavinimas šiuo atveju turėtų būti suprantamas kaip svetimos mokėjimo priemonės užvaldymas ir galėjimas ja naudotis kaip sava. Neteisėtumas suponuoja atlikto veiksmo teisinio pagrindo nebuvimą.

Bankas teigia, kad tretieji asmenys neteisėtu būdu pasisavino pareiškėjo banko naudotojo ID, asmens kodą, mokėjimo kortelės duomenis bei kitus personalizuotus saugos duomenis tik todėl, kad pareiškėjas dėl savo didelio neatsargumo neįvykdė Mokėjimų įstatymo 34 straipsnyje nustatytų mokėtojo pareigų ir neužtikrino, kad, be pareiškėjo, turinčio teisę naudotis mokėjimo priemone, personalizuotais saugumo duomenimis negalėtų pasinaudoti kiti asmenys.

Tiek pareiškėjo, tiek banko paaiškinimai apie mokėjimo operacijos įvykdymo aplinkybes iš esmės sutampa, o banko pateikti sistemų išrašai patvirtina ginčo šalių pateiktus paaiškinimus apie mokėjimo operacijos įvykdymo aplinkybes.

Iš pareiškėjo pateiktų paaiškinimų matyti, kad, pareiškėjas, spausdamas trečiųjų asmenų jam elektroniniu paštu neva VMI atsiųstą aktyvią nuorodą ir vesdamas savo banko atpažinimo ID, asmens kodą bei mokėjimo kortelės duomenis, tikėjosi į savo sąskaitą gauti pinigines lėšas – sumokėtų mokesčių permoką, kurią įprastai grąžina VMI.

Teigdamas, kad pareiškėjo elgesys, dėl kurio jis prarado savo mokėjimo priemonę, turi didelio neatsargumo požymių, bankas remiasi tuo, kad pareiškėjas nesilaikė mokėtojai nustatytos pareigos saugoti personalizuotus saugos duomenis ir niekam jų neatskleisti. Banko teigimu, pareiškėjas savo mokėjimo priemonę naudojo ne pagal sutartyje su pareiškėju sutartą mokėjimo priemonės naudojimo paskirtį, nes norint gauti lėšas į savo sąskaitą nereikia suvesti savo mokėjimo kortelės duomenų ir juo labiau lėšų gavimo patvirtini suvedant „Smart-ID“ PIN1 kodą. Be to, bankas pabrėžė, kad vien tik neatsargus suklastotos aktyvios nuorodos paspaudimas ir netikroje banko interneto svetainėje personalizuotų saugos duomenų bei mokėjimo kortelės duomenų suvedimas būtų nelėmęs pareiškėjo nuostolių dėl mokėjimo operacijos įvykdymo atsiradimo, nes, prieš pareiškėjui suvedant „Smart-ID“ PIN1 kodą, pareiškėjui aiškiai buvo rodoma informacija, koku tikslu pareiškėjo yra prašoma suvesti PIN1 kodą. Vis dėlto pareiškėjas tinkamai nevertino ir šios banko pateiktos informacijos.

Lietuvos bankas pažymi, kad didelis neatsargumas ar paprastas neatsargumas yra vertinamojo pobūdžio aplinkybės, todėl išvada dėl mokėtojo elgesio vertinimo kaip neatsargaus ar labai neatsargaus dėl neautorizuotos mokėjimo operacijos ar dėl mokėjimo priemonės praradimo, lėmusio neautorizuotą mokėjimo operaciją, darytina kiekvienu konkrečiu atveju, įvertinus nustatytų individualių, specifinių aplinkybių visumą, kurią patvirtina ginčo byloje esantys įrodymai ir (arba) yra šalių neginčijamos neautorizuotos mokėjimo operacijos įvykdymo aplinkybės. Taigi, išvada dėl mokėtojo paprasto ar didelio neatsargumo, kaip vertinamojo pobūdžio aplinkybė, negali būti daroma izoliuotai, išsamiai neįvertinus viso neautorizuotos mokėjimo operacijos įvykdymo ir su tuo susijusių aplinkybių konteksto.

Kriterijai, į kuriuos reikėtų atsižvelgti vertinant kaltės laipsnį, yra iš dalies suformuluoti Antrosios mokėjimo paslaugų direktyvos (toliau – PSD2) preambulės 72 punkte: „Siekiant įvertinti galimą mokėjimo paslaugų vartotojo aplaidumą ar didelį aplaidumą, reikėtų atsižvelgti į visas aplinkybes. Įtariamo aplaidumo įrodymai ir laipsnis paprastai turėtų būti vertinami pagal nacionalinę teisę. Tačiau nors aplaidumo sąvoka reiškia, kad pažeidžiamas įsipareigojimas elgtis rūpestingai, didelis aplaidumas turėtų reikšti daugiau nei vien aplaidumą ir apimti labai nerūpestingą elgesį; pavyzdžiui, tai būtų mokėjimo operacijos autorizavimui naudojamų saugumo požymių laikymas prie mokėjimo priemonės atviru ir trečiosioms šalims lengvai atskleidžiamu formatu.“

Didelio neatsargumo sąvoka taip pat plėtojama Lietuvos Aukščiausiojo Teismo praktikoje. Kasacinis teismas yra išaiškinęs, kad „didelis neatsargumas kaip kaltės forma pasireiškia neprotingu arba išskirtiniu rūpestingumo nebuvimu, kai asmuo nėra tiek rūpestingas, kiek akivaizdžiai būtina esamomis aplinkybėmis“.¹

Vertinant, ar pareiškėjo elgesys, kai jis paspaudė trečiųjų asmenų elektroniniu paštu atsiųstą neva VMI aktyvią nuorodą siekdamas į savo banko sąskaitą gauti pinigines lėšas, 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 trečiųjų asmenų neva iš VMI atsiųstas elektroninis laiškas su informacija apie gražinamą sumokėtų mokesčių permoką sutapo su mokesčių deklaravimo pareigos vykdymo laikotarpiu, kai gyventojai visuotinai turėjo pareigą deklaruoti sumokėtus mokesčius ir tuo tikslu prie VMI svetainės dažniausiai jungėsi naudodamiesi interneto banku. Taigi, vien tik šis faktas objektyviai galėjo suklaidinti pareiškėją ir jis pagrįstai galėjo tikėtis, kad, spausdamas jam neva VMI pateiktą aktyvią nuorodą, per savo interneto banką jungiasi prie VMI mokesčių deklaravimo sistemos. Dėl šios priežasties vien fakto, kad pareiškėjas paspaudė jam pateiktą fiktyvią VMI aktyvią nuorodą ir vedė savo personalizuotus saugos duomenis, kurie yra reikalingi prisijungti prie interneto banko paskyros, negalima vertinti kaip labai neatsargaus pareiškėjo elgesio.

Vis dėlto nagrinėjamo ginčo atveju itin svarbus yra faktas, kad pareiškėjo, be duomenų, kurie yra reikalingi prisijungti prie interneto banko paskyros, buvo prašoma suvesti ir mokėjimo kortelės duomenis, juos pareiškėjas nedvejodamas suvedė. Pareiškėjas teigė, kad šiuos duomenis vedė tikėdamasis į savo banko sąskaitą gauti pinigines lėšas. Taigi, pareiškėjas neturėjo tikslo iš savo sąskaitos panaudojant savo mokėjimo kortelės duomenis įvykdyti mokėjimo operaciją, tačiau būtent siekdamas gauti pinigines lėšas į savo banko sąskaitą pareiškėjas suvedė savo mokėjimo kortelės duomenis, t. y. duomenis, kurie yra įprastai suvedami norint inicijuoti ir patvirtinti mokėjimo operaciją iš banko sąskaitos. Be to, prieš pareiškėjui vedant „Smart-ID“ PIN1 kodą, bankas pareiškėjui rodė informaciją, koku tikslu yra prašoma suvesti PIN1 kodą: „patvirtinkite informaciją Norėdami tęsti, įsitikinkite, kad jūsų operacijos informacija yra teisinga Approve this device iPhone (iPhone 13 Pro Max) for app login „Patvirtinti“ „Atšaukti“.

Kaip matyti iš banko pateiktos informacijos, pareiškėjas galėjo pastebėti ir suprasti, kad jo prašoma patvirtinti ne lėšų į banko sąskaitą įskaitymą, o prisijungimą iš *iPhone 13 Pro Max* mobiliojo įrenginio. Svarbu tai, kad pareiškėjo naudojamas mobiliojo telefono įrenginys buvo *Xiomi*, tad net vizualiai pareiškėjas galėjo pastebėti, kad jo prašoma patvirtinti prisijungimą iš kito įrenginio, kuriuo pats pareiškėjas nesinaudojo. Akivaizdu, kad pareiškėjas ir šios banko pateiktos informacijos nevertino kritiškai ir toliau vykdė trečiųjų asmenų nurodymus.

Pažymėtina, kad tam, kad pinigines lėšas būtų gautos į banko sąskaitą, bankai neprašo sąskaitos turėtojo pateikti savo mokėjimo kortelės duomenų ir neprašo suvesti „Smart-ID“ PIN1 kodo. Pareiškėjui faktas, kad, norėdamas į savo sąskaitą gauti pinigines lėšas, jis turėjo suvesti

¹ Lietuvos Aukščiausiojo Teismo 2017 m. balandžio 13 d. nutartis civilinėje byloje Nr. e3K-3-180-378/2017, 29 punktas.

duomenis, kurie iš esmės yra reikalingi atlikti priešingą veiksmą – patvirtinti lėšų iš banko sąskaitos nurašymą, nesukėlė įtarimų ir pareiškėjas vykdė trečiųjų asmenų nurodymus. Pareiškėjui jokių įtarimų nesukėlė ir banko prieš vedant „Smart-ID“ PIN1 kodą rodyta informacija apie tvirtinamą veiksmą. Taigi, pareiškėjas, nors ir turėjo galimybę kritiškai įvertinti savo veiksmų su mokėjimo priemone riziką ir galimas pasekmes, nuo tolimesnių veiksmų nesusilaikė, o priešingai, vykdė visus trečiųjų asmenų nurodymus.

Banko mokėjimo paslaugų teikimo sąlygų (toliau – Sąlygos) 3.3 papunktyje aiškiai reglamentuota, kad banko klientui suteiktų personalizuotų duomenų naudojimas yra skirtas duoti sutikimą įvykdyti mokėjimo operaciją². Ginčo byloje nėra duomenų, kad pareiškėjas būtų buvęs nesupažindintas su Sąlygomis ar kad būtų jų nesupratęs. Taigi, pareiškėjas iš esmės galėjo suprasti, kad tiek mokėjimo kortelės duomenų suvedimas, tiek „Smart-ID“ PIN kodo naudojimas gali lemti tam tikras teises pasekmes, šiuo atveju – mokėjimo priemonės praradimą ir neautorizuotos mokėjimo operacijos iš jo banko sąskaitos įvykdymą.

Lietuvos banko nuomone, jeigu pareiškėjas būtų buvęs pakankamai kritiškas savo su mokėjimo priemone atliekamų veiksmų atžvilgiu ir būtų kritiškai vertinęs bent vieną iš jo atliktų veiksmų ir susilaikęs nuo veiksmų atlikimo, jis būtų galėjęs išvengti neautorizuotos mokėjimo operacijos iš savo sąskaitos įvykdymo. Jeigu pareiškėjas dėl objektyvių aplinkybių galėjo ir nesuprasti, kad elektroninį laišką su aktyvia nuoroda jam siuntė ne VMI, o sukčiai, tačiau pareiškėjas turėjo galimybę suprasti, kad jo prašoma atlikti veiksmus, kurių nėra įprastai prašoma atlikti norint pinigines lėšas gauti į savo sąskaitą, o priešingai – yra prašoma atlikti veiksmus, kurie įprastai yra atliekami norint įvykdyti mokėjimo operacijas iš banko sąskaitos. Be to, pareiškėjas, prieš suveddamas „Smart-ID“ PIN1 kodą, jam banko pateiktoje informacijoje galėjo pastebėti, kad šį veiksmą jo prašoma atlikti visai kitu, nei jis tikisi, tikslu.

Lietuvos banko nuomone, jeigu pareiškėjas bent vieną iš jo atliekamų veiksmų būtų įvertinęs kritiškai, būtų galėjęs išvengti nuostolių dėl neautorizuotos mokėjimo operacijos įvykdymo. Vis dėlto atlikdamas veiksmus pareiškėjas atidžiai nevertino jam pateiktos informacijos ir nekreipdamas tinkamo dėmesio 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 mokėjimo operaciją.

Mokėjimų įstatymo 34 straipsnyje reglamentuojamos mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigos: 1) naudotis mokėjimo priemone pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas; 2) sužinojus apie mokėjimo priemonės praradimą, vagystę arba neteisėtą pasisavinimą ar neautorizuotą jos naudojimą, nedelsiant apie tai pranešti mokėjimo paslaugų teikėjui arba jo nurodytam subjektui. Mokėjimo paslaugų vartotojas, gavęs mokėjimo priemonę, privalo imtis veiksmų, kad būtų apsaugoti personalizuoti saugumo duomenys (2 dalis).

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 mokėjimo operacija iš pareiškėjo sąskaitos ir pareiškėjas patyrė nuostolių.

Mokėjimų įstatymo 39 straipsnio 3 dalyje nustatyta, kad mokėtoju 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.

² Atsiskaitant mokėjimo kortele, tam tikrais atvejais Klientas (Mokėtojas) ar jo atstovas Sutikimą taip pat gali patvirtinti pateikdamas mokėjimo kortelės duomenis (pvz.: vardas ir pavardė / pavadinimas, kortelės numeris, galiojimo terminas, CVV2/CVC2 kodas (skaitmenys kitoje mokėjimo kortelės pusėje)), ar Klientui (Mokėtojui) nustatytu eiliškumu atliekant tam tikrus veiksmus (pvz.: mokėjimo kortelės įdėjimas į tam skirtą vietą, konkrečios paslaugos ar prekės užsakymas), kurie jam siūlomi atsiskaitymo vietose, ar pateikdamas Sutikimą kitu būdu, nurodytu konkrečios Mokėjimo paslaugos teikimo sąlygose ar kitoje Sutartyje“.

Įvertinus pirmiau išdėstytą informaciją, konstatuotina, kad yra pagrindas pareiškėjui taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, todėl pareiškėjo reikalavimas bankui grąžinti bent dalį neautorizuotos mokėjimo operacijos lėšų sumą yra nepagrįstas ir atmestinas.

2. Dėl mokėjimo nurodymo įvykdyti mokėjimo operaciją atšaukimo

Pareiškėjas teigė, kad bankas turėjo nevykdyti mokėjimo operacijos ir ją atšaukti, nes tuo metu, kai pareiškėjas kreipėsi į banką dėl mokėjimo operacijos atšaukimo, mokėjimo operacijos lėšos pareiškėjo banko sąskaitoje dar buvo tik rezervuotos.

Vertinant banko pareigos atšaukti mokėjimo operacijas vykdymą, pažymėtina, kad, pagal Mokėjimų įstatymo 44 straipsnio 1 dalies nuostatas, mokėjimo paslaugų vartotojas negali atšaukti mokėjimo nurodymo po to, kai jį gauna mokėtojo mokėjimo paslaugų teikėjas, išskyrus šiame straipsnyje nustatytas išimtis. Minėto Mokėjimų įstatymo straipsnio 4 dalyje taip pat nustatyta, kad, pasibaigus 1 dalyje nurodytam laikotarpiui, mokėjimo nurodymas gali būti atšauktas tik tuo atveju, kai dėl to susitaria mokėjimo paslaugų vartotojas ir atitinkamas mokėjimo paslaugų teikėjas, o šio straipsnio 2 dalyje numatytais atvejais būtinas ir gavėjo sutikimas. Mokėjimo paslaugų teikėjas gali imti komisinį atlyginimą už mokėjimo nurodymo atšaukimą, jeigu tai numatyta bendrojoje sutartyje.

Taigi, pasibaigus Mokėjimų įstatymo 44 straipsnio 1 dalyje nurodytam terminui, mokėjimo nurodymas gali būti atšauktas tik dėl to susitarus vartotojui ir jo mokėjimo paslaugų teikėjui, todėl nurodytos galimybės (t. y. mokėjimo nurodymo atšaukimo) įtvirtinimas Mokėjimų įstatyme neturėtų būti vertinamas kaip priverstinis lėšų grąžinimas mokėtojui, esant jo atitinkamam prašymui (pasibaigus 44 straipsnio 1 dalyje nurodytam terminui).

Remiantis ginčo byloje esančiais duomenimis, pareiškėjo prašymas atšaukti mokėjimo operaciją bankui buvo pateiktas po to, kai mokėjimo nurodymą jau buvo gavęs bankas, todėl Mokėjimų įstatyme nustatytas mokėjimo nurodymo atšaukimo terminas jau buvo praėjęs ir bankas atšaukti pareiškėjo vardu pateikto mokėjimo nurodymo nebegalėjo.

Atsižvelgiant į tai, kas buvo išdėstyta pirmiau, nėra pagrindo vertinti, kad bankas nepagrįstai įvykdė mokėjimo operaciją ir kad nepagrįstai jos neatšaukė.

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 Lietuvos banko 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