



**LIETUVOS BANKO  
TEISĖS IR LICENCIJAVIMO DEPARTAMENTO  
DIREKTORIUS**

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

2023-08-30 Nr. 429-455  
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 4 d. iš pareiškėjo sąskaitos banke pareiškėjui banko išduota mokėjimo kortele panaudojant *Google Pay* mokėjimo operacijos patvirtinimo metodą buvo inicijuota ir patvirtinta 624,98 Eur mokėjimo operacija (toliau – mokėjimo operacija) lėšų gavėjui *Micromania Villable* (toliau – gavėjas). Mokėjimo operacija buvo įvykdyta pareiškėjo mokėjimo kortelę pridėjus prie *Google Pay*, įdiegto kitame mobiliojo telefono įrenginyje.

Bankui atsisakius pareiškėjui gražinti mokėjimo operacijos sumą, pareiškėjas kreipėsi į Lietuvos banką prašydamas išnagrinėti vartojimo ginčą ir gražinti visą mokėjimo operacijos sumą. Pareiškėjas paaiškino, kad 2023 m. balandžio 2 d. užsisakė avalynę iš internetinės parduotuvės ne Lietuvoje. „2023 m. balandžio 3 d. gavau sms žinutę iš *DHL*, kurioje buvo prašoma koreguoti pristatymo adresą, nes jis blogai suvestas. Prieš gerą pusmetį keitėme savo gatvės, kurioje gyvename, pavadinimą, todėl ne kartą pasitaikė atvejis, kad kurjeriai neranda naujos gatvės pavadinimo sąrašė ir kartais paprašo atnaujinti informaciją. Todėl 2023 m. balandžio 3 d. vakare paspaudžiau nuorodą žinutėje. Nuoroda nuvedė į *DHL* puslapį kaip dabar jau tikėtina, jis buvo netikras. Nuorodoje suvedžiau naują adresą ir už šią adresą atnaujinimo paslaugą buvo paprašyta sumokėti 3,47 Eur. Patvirtinau, kad apmokėti sutinku. Atliekant mokėjimą, manęs paprašė suvesti kodą, kurį atsiuntė SMS žinute. Žinutė atėjo iš Swedbank, kurioje buvo informacija, kad mano kreditinė kortelė, kuria noriu atlikti mokėjimą, yra pridėta prie *Google Pay* ir kartu atsiųstas kodas apmokėjimui užbaigti. Kodą suvedžiau ir mokėjimą atlikau. Akcentuoju, kad Swedbank atsiųstoje SMS žinutė buvo skirta užbaigti operacijai ir joje nėra nieko indikuojančio, kad toks mokėjimas ar kortelės pridėjimas prie *Google Pay* yra įtartinas, pavojingas ar pan. <...>. Sekančia dieną, 2023 m. balandžio 4 d. vakare pastebėjau, kad iš mano kredito kortelės buvo atliktas mokėjimas sumai 624,98 Eur. Pinigai kortelėje buvo rezervuoti. Pats jokio mokėjimo neinicijavau, netvirtinau ir jokios operacijos neatlikau.“ Pareiškėjo teigimu, kai kreipėsi į banką dėl mokėjimo operacijos atšaukimo, mokėjimo operacijos lėšos jo sąskaitoje buvo tik rezervuotos, todėl bankas galėjo šias lėšas pareiškėjui sugražinti. Pareiškėjo teigimu, mokėjimo operacija buvo įvykdyta dėl banko kaltės, nes bankas jos neatšaukė laiku.

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, mokėjimo operacija buvo įvykdyta pareiškėjo mokėjimo kortelę susiejus su skaitmenine pinigine (*Google Pay*), kortelės susiejimą patvirtinus suvedant banko pareiškėjui mobiliuoju telefonu SMS žinute išsiųstą vienkartinį saugos kodą. Bankas pažymėjo, kad pareiškėjas iš trečiųjų asmenų gavo pranešimą su aktyvia nuoroda, kur jo buvo prašoma sumokėti 3,47 Eur neva už siuntos pristatymo adresą atnaujinimą, šiuo tikslu pareiškėjas suvedė savo mokėjimo kortelės duomenis, tačiau tretieji asmenys juos nusavino ir panaudojo pareiškėjo mokėjimo kortelę pridėdamas prie *Google Pay*. Banko teigimu, tretieji asmenys pasinaudodami nusavintais pareiškėjo mokėjimo kortelės duomenimis nebūtų galėję inicijuoti mokėjimo operacijos, jeigu pareiškėjas jiems nebūtų perdavęs banko pareiškėjui SMS žinute siųsto

vienkartinio saugos kodo.

Bankas taip pat pažymėjo, kad po to, kai pareiškėjui išsiuntė SMS žinutę su vienkartinio saugos kodu, papildomai į pareiškėjo mobiliajame telefone įdiegtą banko mobiliąją programėlę išsiuntė pranešimą, kad pareiškėjo mokėjimo kortelė yra pridėta prie *Google Pay*, tačiau pareiškėjas į šią žinutę nekreipė jokio dėmesio, nors mokėjimo operacija buvo įvykdyta tik po 26 valandų nuo šios žinutės išsiuntimo. Banko nuomone, jeigu pareiškėjas būtų buvęs atidus ir būtų kritiškai įvertinęs tiek savo veiksmus su savo mokėjimo priemone, taip pat būtų kreipęs tinkamą dėmesį į banko jam siųstus pranešimus, net ir paspaudęs aktyvią nuorodą pareiškėjas būtų turėjęs galimybę išvengti neautorizuotos mokėjimo operacijos iš jo banko sąskaitos įvykdymo. Be to, bankas pažymėjo, kad pareiškėjui pavyko išvengti didesnių nuostolių, nes banko sistemos apribojo paskesnes dvi mokėjimo operacijas kaip įtartinas ir jų neįvykdė.

Pasisakydamas dėl pareiškėjo argumento, kad dėl banko kaltės mokėjimo operacijos vykdymas nebuvo atšauktas, bankas paaiškino, kad neturi galimybės atšaukti mokėjimo operacijos po to, kai mokėjimo nurodymas yra gautas banke. Pareiškėjas dėl mokėjimo operacijos atšaukimo kreipėsi po to, kai mokėjimo nurodymas buvo gautas banke.

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.

Pareiškėjo ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjui pareiškėjo vardu banke atidarytoje sąskaitoje kortele atliktos mokėjimo operacijos lėšas, iš viso 624,98 Eur. Pareiškėjas teigia neautorizavęs mokėjimo operacijos, tačiau pripažįsta trečiųjų asmenų suklastotame *DHL* interneto puslapyje suvedęs savo mokėjimo kortelės duomenis ir tretiesiems asmenims perdavęs banko jam SMS žinutę siųstą vienkartinį saugos kodą, skirtą mokėjimo kortelei prie *Google Pay* pridėti. Pareiškėjo teigimu, bankas pareiškėjo SMS žinutėje, skirtoje mokėjimo kortelei prie *Google Pay* pridėti, neįspėjo, kad mokėjimo kortelės pridėjimas prie *Google Pay* gali būti pavojingas. Pareiškėjas taip pat teigia, kad mokėjimo operacija buvo įvykdyta dėl banko kaltės, nes tada, kai buvo kreiptasi į banką dėl mokėjimo operacijos atšaukimo, lėšos pareiškėjo banko sąskaitoje buvo dar tik rezervuotos, todėl bankas turėjo nevykdyti mokėjimo operacijos.

Bankas teigia, kad pareiškėjo mokėjimo operacija buvo patvirtinta šalių sutarta forma ir tvarka, dėl to bankas ją pagrįstai įvykdė. Taip pat bankas teigia, kad yra sąlygos pareiškėjo elgesi, prarandant savo mokėjimo priemonę, vertinti kaip labai neatsargų, todėl 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. Atsiliepime 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 gražinimą*

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 nesąžiningai (1 punktas).

Mokėjimų įstatymo 39 straipsnio 3 dalyje nustatyta, kad mokėtojai tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai, jeigu jis juos patyrė veikdamas nesąžiningai arba tyčia ar dėl didelio neatsargumo neįvykdęs vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų. 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 galėjo pasisavinti pareiškėjo 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 saugos 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 SMS žinute neva *DHL* atsiųstą aktyvią nuorodą ir vesdamas savo mokėjimo kortelės duomenis, įskaitant ir CVC kodą bei SMS žinute banko siųstą vienkartinį saugos kodą, tikėjosi patvirtinti 3,47 Eur mokėjimo operaciją už siuntos pristatymo adreso pakeitimą.

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 nekreipė tinkamo dėmesio į banko SMS žinutėje su vienkartinio saugos kodu pateiktą informaciją apie šio kodo naudojimo paskirtį ir tai, kad šio kodo paskirtis neatitiko pareiškėjo siekiamo atlikti veiksmo su savo mokėjimo priemone tikslo – įvykdyti 3,47 Eur mokėjimo operaciją.

Be to, bankas atkreipė dėmesį, kad nuo pareiškėjo mokėjimo kortelės pridėjimo prie *Google Pay* iki mokėjimo operacijos įvykdymo praėjo net 26 valandos, taigi, pakankamas laiko tarpas, per kurį pareiškėjas galėjo apsvarstyti savo atliktus veiksmus ir banko jam siųstą informaciją. Tačiau pareiškėjas nekreipė deramo dėmesio nei į atliekamus veiksmus su mokėjimo priemone, nei į banko siunčiamus pranešimus ir juose pateikiamą informaciją, susijusią su pareiškėjo mokėjimo priemonės naudojimo tikslu. Bankas pabrėžė, kad vien tik neatsargus suklastotos aktyvios nuorodos paspaudimas ir netikroje interneto svetainėje mokėjimo kortelės duomenų suvedimas būtų nelėmęs pareiškėjo nuostolių dėl mokėjimo operacijos įvykdymo atsiradimo, mokėjimo kortelei prie *Google Pay* pridėti kitame įrenginyje buvo būtinas papildomas saugos kodas. Pareiškėjui banko siųstoje SMS žinutėje su vienkartinio saugos kodu buvo aiškiai atskleista vienkartinio saugos kodo naudojimo paskirtis – pridėti mokėjimo kortelę prie *Google Pay*. 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.“<sup>1</sup>

Vertinant, ar pareiškėjo elgesys, kai jis paspaudė trečiųjų asmenų atsiųstą neva *DHL* siųstą aktyvią nuorodą siekdamas apmokėti už siuntos pristatymo adreso pakeitimą, 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 vien tik sukčių atsiųstos aktyvios nuorodos paspaudimas nėra laikomas itin neatsargiu mokėtojo elgesiu, nes dažnai sukčių suklastotos aktyvios nuorodos vizualiai būna gana panašios į tikrąsias interneto svetaines ir vartotojui, neturinčiam specialiųjų žinių, gali būti sudėtinga įvertinti atsiųstos nuorodos tikrumą. Pareiškėjo Lietuvos bankui iš trečiųjų asmenų atsiųstoje SMS žinutėje buvo pateikiama tokia informacija: „*DHL: Užsakymo metu įvestas neteisingas pristatymo adresas prašome atnaujinti informaciją deliverypacdel.com.*“

Svarbu pažymėti, kad sukčiavimo atvejis, į kurį pateko pareiškėjas, nėra naujas, su panašiomis sukčiavimo schemomis vartotojai susiduria ne vienus metus ir apie panašias sukčiavimo schemas yra paskelbta nemažai viešai prieinamos informacijos. Iš pareiškėjo Lietuvos bankui pateiktos trečiųjų asmenų žinutės galima matyti, kad nors žinutė buvo parašyta lietuviškais rašmenimis, tačiau, jeigu tik būtų neskubėjęs vykdyti trečiųjų asmenų nurodymų ir tinkamai vertinęs žinutės turinį, pareiškėjas būtų pastebėjęs, kad žinutė apie neteisingą adreso įvedimą neva iš kurjerio atėjo kitą dieną po prekės elektroninėje parduotuvėje įsigijimo, nors įprastai siuntų pristatymas trunka bent keletą dienų. Be to, jeigu pristatymo adresas yra neteisingas, t. y. siuntos gavėjo tuo adresu negalima rasti, tai turėtų paaiškėti jau pačios siuntos pristatymo metu.

Įvertinus tiek gautos žinutės turinį, tiek joje prašomų atlikti veiksmų pagrįstumą, galima vertinti, kad pareiškėjas galėjo pastebėti ir įtarti, kad prieš jį gali būti vykdoma sukčiavimo ataka, todėl galėjo susilaikyti nuo aktyvios nuorodos spaudimo ir savo mokėjimo kortelės duomenų suvedimo. Be to, svarbu atkreipti dėmesį, kad siuntų pervežimo bendrovės *DHL* puslapyje pateikiama informacija, kad siuntos pristatymo adreso keitimas šioje bendrovėje nėra galimas. Tad jeigu tik pareiškėjas būtų neskubėjęs vykdyti trečiųjų asmenų nurodymų ir pasitikrinęs informaciją oficialiame *DHL* puslapyje, tikėtina, būtų išvengęs aktyvios nuorodos paspaudimo ir savo mokėjimo kortelės duomenų suvedimo.

Nagrinėjamo ginčo atveju svarbus yra faktas, kad pareiškėjo, be mokėjimo kortelės duomenų, buvo prašoma suvesti ir banko pareiškėjui SMS žinute siųstą vienkartinį saugos kodą, nors SMS žinutėje nurodyta saugos kodo paskirtis – mokėjimo kortelę pridėti prie *Google Pay*, bet ne patvirtinti mokėjimo operaciją, kaip teigė manęs pareiškėjas. Banko pateiktais duomenimis, pareiškėjui minėtoje SMS žinutėje buvo pateikiama tokia informacija: „*Jūsų kortelės pridėjimo prie Google Pay patvirtinimo kodas yra XXXXXX. Šis kodas galioja 30 minučių.*“

Kaip matyti, banko pateiktoje SMS žinutėje nebuvo jokios informacijos apie pareiškėjo tvirtinamą mokėjimo operaciją, o priešingai – buvo aiškiai nurodyta, kad šis kodas yra skirtas

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

mokėjimo kortelei prie *Google Pay* pridėti. Taigi, pareiškėjui nesukėlė įtarimo nei faktas, kad įprastai, mokėjimo operacijas atliekant mokėjimo kortele, bankas nesiunčia vienkartinio saugos kodo, nei tai, kad SMS žinutėje buvo pateikta informacija apie kitokią šio kodo naudojimo paskirtį, nei tuo metu galėjo manyti pareiškėjas. Akivaizdu, kad pareiškėjas šios banko pateiktos informacijos nevertino kritiškai ir toliau vykdė trečiųjų asmenų nurodymus.

Nagrinėjamo ginčo situacijoje svarbu pažymėti ir tai, kad bankas 2023 m. balandžio 3 d. papildomai pareiškėjui į jo mobiliajame telefone įdiegtą banko programėlę atsiuntė pranešimą, kad „*Jūsų kortelė \*\*\* 3869 paruošta „Google Pay“ bekontakčiams atsiskaitymams internetu.*“ Tačiau pareiškėjas ir į šią banko žinutę nekreipė dėmesio, nors turėjo pakankamai laiko, nes mokėjimo operacija iš pareiškėjo sąskaitos buvo įvykdyta tik po 26 valandų nuo šios banko žinutės išsiuntimo. Taigi, pareiškėjas turėjo pakankamai laiko įvertinti tiek savo atliktų veiksmų su savo mokėjimo priemone pagrįstumą, tiek banko jam pateiktos informacijos turinį. Jeigu pareiškėjas būtų tinkamai įvertinęs banko jam siųstą informaciją ir ėmęsis bent kokių nors veiksmų, kad išsiaiškintų banko jam siunčiamų pranešimų tikslą, nepaisant to, kad paspaudė aktyvią nuorodą ir joje suvedė savo mokėjimo kortelės duomenis, pareiškėjas dar būtų galėjęs išvengti neautorizuotos mokėjimo operacijos iš jo sąskaitos įvykdymo. Tačiau pareiškėjas, nors ir turėjo galimybę kritiškai įvertinti jam pateiktą informaciją, to nepadarė.

Lietuvos banko nuomone, jeigu pareiškėjas būtų buvęs pakankamai kritiškas savo su mokėjimo priemone atliekamų veiksmų atžvilgiu ir būtų kritiškai vertinęs ne tik sukčių jam pateiktą informaciją apie mokėjimo operacijos tikslą, bet ir banko jam pateiktą informaciją apie mokėjimo priemonės naudojimo paskirtį, jis būtų galėjęs išvengti neautorizuotos mokėjimo operacijos iš savo sąskaitos įvykdymo. Pareiškėjas, prieš suveddamas SMS žinute gautą vienkartinį saugos kodą, jam banko pateiktoje informacijoje galėjo pastebėti, kad šį veiksma jį prašoma atlikti visai kitu, nei jis tikisi, tikslu, ir netgi šį kodą suvedęs turėjo dar pakankamai laiko įvertinti jam banko pateiktą informaciją ir kreiptis į banką pasitikslinti, kokiu tikslu jam bankas atsiuntė pranešimą apie mokėjimo kortelės pridėjimą prie *Google Pay*.

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 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 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 gražinimas 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