LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

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

2026-05-08 Nr. 429-147
Vilnius

Lietuvos bankas gavo pareiškėjo 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:

2026 m. sausio 5 d. 15:02 val. iš pareiškėjo sąskaitos banke pareiškėjui banko išduota *Mastercard* mokėjimo kortele (toliau – Kortelė) buvo inicijuota 1 868,82 EUR mokėjimo operacija (toliau – ginčijamas mokėjimas) lėšų gavėjai IDEAL (toliau – lėšų gavėja). Ginčijamas mokėjimas buvo inicijuotas pareiškėjo mokėjimo kortelę pridėjus prie mobiliųjų mokėjimų sistemos *Apple Pay* (toliau – *Apple Pay*) trečiųjų asmenų įrenginyje. 2026 m. sausio 5 d. 15:04 val. pareiškėjas Kortelę užblokavo savo interneto banke.

2026 m. sausio 5 d. pareiškėjas kreipėsi į banką ir informavo apie sukčiavimo ataką. Pareiškėjas paaiškino, kad gavo du SMS pranešimus[1] su juose pateiktomis netikromis aktyviomis nuorodomis, ir pasidalino ekrano vaizdo kopijomis. Pateikti duomenys rodo, kad tretieji asmenys išgavo iš pareiškėjo Kortelės duomenis ir vienkartinį kodą[2], reikalingą Kortelei prie *Apple Pay* sistemos pridėti. Pareiškėjas nurodė, jog ginčijamo mokėjimo neautorizavo, ir prašė grąžinti lėšas, inicijuojant lėšų grąžinimą (angl. *chargeback*) pagal *Mastercard* organizacijos lėšų grąžinimo gidą (angl. *Chargeback Guide*)[3] (toliau – *Mastercard* taisyklės).

2026 m. sausio 7 d. bankas atsisakė tenkinti lėšų grąžinimo prašymą bei atlyginti pareiškėjo nuostolius dėl ginčijamo mokėjimo. Bankas paaiškino, kad mokėjimo operacija negali būti laikoma neautorizuota – ginčijamas mokėjimas buvo atliktas naudojantis *Apple Pay*, pareiškėjui su trečiaisiais asmenimis pasidalinus Kortelės duomenimis ir vienkartiniu saugos kodu.

Pareiškėjas, nesutikdamas su banko sprendimu, kreipėsi į Lietuvos banką dėl vartojimo ginčo nagrinėjimo. Kreipimesi į Lietuvos banką pareiškėjas nurodė tapačias aplinkybes, kokios buvo nurodytos bankui. Pareiškėjas prašė įpareigoti banką grąžinti ginčijamo mokėjimo sumą – 1 868,82 EUR.

Atsiliepime bankas nurodė nesutinkantis su pareiškėjo reikalavimu ir prašė jį atmesti. Bankas neginčijo aplinkybės, kad ginčijamas mokėjimas buvo neautorizuotas, tačiau papildomai nurodė, kad pareiškėjo veiksmams būdingas didelis neatsargumas, todėl bankas negali būti įpareigotas grąžinti ginčijamo mokėjimo sumos.

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

---

[1] Pareiškėjo įvardintus kaip angl. „*fake delivery and parking payment reminders*“.

[2] Pateiktais duomenimis, 2026 m. sausio 5 d. 14:52 val. pareiškėjas prisijungė prie savo interneto banko iš savo įprastai naudojamo išmaniojo įrenginio, o banko jam pateiktame pranešime nurodyta: *„Your security code for **adding the card to Apple Pay** is 486551. The code will be active for 30 minutes. Important! **This code is not intended for payment confirmation.** Enter the code only in the Apple Pay. **Don't disclose this code to anyone.**“* Norėdamas sužinoti vienkartinį saugos kodą kodo galiojimo laikotarpiu tik pareiškėjas asmeniškai buvo prisijungęs prie savo interneto banko aplinkos.

[3] https://www.mastercard.us/content/dam/mccom/global/documents/chargeback-guide.pdf.

banke taisyklių (toliau – Taisyklės) 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.

Pareiškėjo ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjui ginčijamo mokėjimo lėšas.

Ginčo šalys iš esmės nesutaria dėl to, ar bankas turi pareigą pareiškėjui grąžinti įvykdyto ginčijamo mokėjimo sumą. Pareiškėjas neigia inicijavęs Kortelės pridėjimą prie *Apple Pay* sistemos ir inicijavęs ginčijamą mokėjimą, tačiau teigia, kad buvo suklaidintas trečiųjų asmenų dėl Kortelės duomenų ir saugos kodo perdavimo – pareiškėjas nesiekė Kortelės pridėti prie *Apple Pay* sistemos, tik apmokėti paslaugą.

Siekiant išspręsti tarp pareiškėjo ir banko kilusį ginčą, Lietuvos banko vertinimu, būtina nustatyti, ar bankas: 1) turi pareigą grąžinti pareiškėjui įvykdyto ginčijamo mokėjimo sumą; 2) pagrįstai atsisakė ginčijamo mokėjimo atžvilgiu pradėti lėšų grąžinimo pagal Mastercard taisykles procedūrą.

1. Dėl banko pareigos grąžinti pareiškėjui ginčijamo mokėjimo sumą

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.

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.

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 neautorizuotų mokėjimo operacijų 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 neatsargumas, dėl kurio su mokėjimo operacijų 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 aplinkybėmis. Didelis mokėtojo neatsargumas gali būti konstatuojamas tik tuomet, jei mokėtojas elgėsi labai nerūpestingai. Aplinkybę, kad mokėtojas

elgėsi labai nerūpestingai, turi įrodyti mokėjimo paslaugų teikėjas, pateikdamas konkrečius tokį elgesį pagrindžiančius įrodymus. Ši įrodinėjimo našta negali būti perkelta mokėtojui.

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, todėl šiame sprendime bus pasisakoma tik šiai konkrečiai ginčo bylai aktualiais aspektais.

Neautorizuotų mokėjimo operacijų 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 neatsargumo.

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 ginčijamo mokėjimo pareiškėjas patyrė dėl savo didelio neatsargumo, t. y. pareiškėjas, perduodamas tretiesiems asmenims Kortelės duomenis ir vienkartinį jos susiejimo su *Apple pay* kodą, įgalino trečiuosius asmenis prijungti Kortelę prie *Apple pay* sistemos naujame įrenginyje ir leido tretiesiems asmenims susikurti skaitmeninę Kortelės versiją su galimybe pagal *Apple* taisykles vykdyti pareiškėjo tapatybės patvirtinimą saugesniu būdu. Banko teigimu, pareiškėjas pats atsidarė fiktyvią (sukurtą sukčių) interneto svetainę, kurios adresas akivaizdžiai neatitiko originalios svetainės adreso, tuomet įvedė į ją Kortelės duomenis ir vienkartinį saugos kodą. Taip pareiškėjas suteikė tretiesiems asmenims galimybę aktyvuoti Kortelę jų įrenginyje ir sukurti Kortelės skaitmeninę versiją, todėl tretieji asmenys galėjo atlikti ginčijamą mokėjimą.

Banko sprendimas nekompensuoti pareiškėjo nuostolių dėl neautorizuoto ginčijamo mokėjimo įvykdymo galėtų būti vertinamas kaip pagrįstas tik tada, jeigu būtų įrodyta, kad pareiškėjas, atskleisdamas tam tikrus personalizuotus savo mokėjimo priemonių saugumo duomenis, leido tretiesiems asmenims perimti savo sąskaitos valdymą ir šių veiksmų pagrindu tretieji asmenys galėjo inicijuoti ginčijamą mokėjimą, t. y. elgėsi itin aplaidžiai – buvo labai neatsargus.

Lietuvos bankas, siekdamas nustatyti, ar pareiškėjo elgesys šiuo atveju gali būti laikomas labai neatsargiu, vertino visų atliktų veiksmų visumą, t. y. jo elgesį paspaudžiant jam trečiųjų asmenų atsiųstą aktyvią nuorodą, suvedant savo mokėjimo priemonės personalizuotus saugumo duomenis suklastotame interneto banko puslapyje bei patvirtinant atliekamus veiksmus, pateikiant ir Kortelės pridėjimo prie *Apple Pay* kodą, 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, jo personalizuotų saugumo žymenų suvedimo ir atskleidimo reikšme bei teisinėmis pasekmėmis.

Vertinant paties pareiškėjo elgesį, svarbu nustatyti, kaip pareiškėjas, kaip mokėjimo paslaugų vartotojas, buvo įtikintas atskleisti savo mokėjimo priemonės personalizuotus saugos duomenis, įgalinusius trečiuosius asmenis inicijuoti ginčijamą mokėjimą.

Lietuvos bankas, įvertinęs pareiškėjo kreipimesi ir banko atsiliepime nurodytas aplinkybes bei kartu su kreipimusi ir atsiliepimu pateiktus duomenis, nustatė, kad prieš ginčijamo mokėjimo įvykdymą pareiškėjas iš trečiųjų asmenų gavo aktyvią nuorodą, jis buvo skatinamas ją paspausti ir suvesti savo personalizuotus saugos duomenis, kad neva sumokėtų už parkavimosi paslaugas. Kaip vėliau paaiškėjo, pareiškėjas, paspaudęs trečiųjų asmenų jam atsiųstą aktyvią nuorodą, pateko į suklastotą interneto puslapį, jame suvedė tik jam žinomus asmeninius duomenis, šie buvo nusavinti trečiųjų asmenų (sukčių) ir panaudoti tam, kad Kortelė būtų prijungta prie *Apple Pay* trečiųjų asmenų įrenginyje ir būtų sukurta jos skaitmeninė versija. Pridėjimo prie *Apple Pay* kodas, kurį bankas sugeneravo tik po pareiškėjo sėkmingos autentifikacijos vienkartinio kodo galiojimo laikotarpiu, yra personalizuota saugumo priemonė, naudojama mokėjimo priemonei aktyvuoti. Byloje turimais duomenimis, pareiškėjas prisijungė

prie savo interneto banko paskyros, sužinojo vienkartinį pridėjimo prie *Apple Pay* kodą ir juo pasidalino su trečiaisiais asmenimis, suvesdamas jį suklastotoje svetainėje, siekdamas sumokėti už automobilio parkavimą.

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.

2024 m. gruodžio 10 d. pareiškėjo ir banko sudarytos Kredito kortelės sutarties (toliau – Kortelės sutartis) 9.8 papunktyje nustatyta, kad „*Naudotojas privalo atidžiai tikrinti jam pateikiamus pranešimus, susijusius su Operacijų patvirtinimu Tapatybės patvirtinimo priemonėmis (pvz., įsitikinti, kad pranešimo jo išmaniajame įrenginyje turinys sutampa su jo atliekama Operacija), ir nustatęs neatitikimus ar kitu būdu suabejojęs tvirtinamos Operacijos tikrumu, privalo susilaikyti nuo jos tvirtinimo. Bankas primygtinai rekomenduoja neatlikti jokių Operacijų, kurios inicijuojamos paspaudus SMS ar kitu būdu gautą nuorodą, prieš tai neįsitikinus, kad pranešimą su nuoroda atsiuntė tikrai Bankas. Naudotojas privalo laikytis kitų Banko nurodytų sukčiavimo prevencijos rekomendacijų, skelbiamų Banko tinklalapyje ar Banko pateikiamų kitu būdu.*"

Banko ir pareiškėjo santykius reglamentuojančių banko Mokėjimo paslaugų teikimo taisyklių (toliau – Taisyklės) 22 punkte 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.

Banko ir pareiškėjo santykius reglamentuojančių banko Elektroninių paslaugų teikimo sutarties sąlygų (toliau – Sąlygos) 8 skyriuje reglamentuojama tapatybės patvirtinimo priemonės ir mokėjimo operacijų tvirtinimo ir (arba) pasirašymo procedūra, o 16 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.

Taigi, pirmiau aptartos Kortelės sutarties, Taisyklių ir Sąlygų nuostatos aiškiai ir nedviprasmiškai nustato tapatybės patvirtinimo priemonės personalizuotų saugumo duomenų naudojimo mokėjimo operacijų vykdymo procese paskirtį ir jų panaudojimo galimas pasekmes mokėtojui, aiškiai ir nedviprasmiškai apibrėžia, kad už šių duomenų konfidencialumo išsaugojimą yra atsakingas mokėtojas, šiuo atveju – pareiškėjas.

Atsižvelgiant į tai, manytina, kad pareiškėjo elgesys būtų laikomas kaip atitinkantis mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, jei būtų nustatyta, jog pareiškėjas ėmėsi pakankamų veiksmų (arba priešingai – nustačius, kad nuo tam tikrų veiksmų susilaikė) tam, kad jam banko išduotų mokėjimo priemonių personalizuotų saugumo duomenų, įgalinančių inicijuoti ir tvirtinti mokėjimus, konfidencialumas būtų tinkamai užtikrintas, o jam banko išduota mokėjimo priemonė būtų naudojama šalių sutartinius santykius reglamentuojančių dokumentų nustatyta tvarka bei sąlygomis.

Vertinant, ar pareiškėjo elgesys, kai jis, gavęs trečiųjų asmenų aktyvią nuorodą į neva *Unipark* puslapį, suklastotoje svetainėje suvedė savo asmeninius bei Kortelės duomenis ir vienkartinį Kortelės pridėjimo prie *Apple Pay* kodą, kad jį sužinotų, pareiškėjas papildomai turėjo prisijungti prie savo interneto banko, ir taip leido tretiesiems asmenims jų valdomame įrenginyje susikurti skaitmeninę Kortelės versiją, 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, jog 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.

Nagrinėjamo ginčo atveju prieš pareiškėją nukreipta sukčiavimo ataka buvo ne nauja, o gana plačiai žinoma, nes periodiškai skelbiama nemažai viešai prieinamos informacijos, įspėjančios vartotojus apie panašias sukčiavimo atakas ir raginančios juos būti budrius, nespausti aktyvių nuorodų ir nevesti savo personalizuotų saugos duomenų.

Banko Lietuvos bankui pateiktais duomenimis, bankas informaciją apie sukčiavimo atakas skelbė savo interneto banko puslapyje, SMS žinutėmis, be to, 2025 m. spalio 24 d. interneto banko žinute asmeniškai pareiškėjui priminė apie padažnėjusius sukčiavimo atvejus ir paaiškino, kaip atpažinti sukčiavimo veiksmus. Kaip minėta, nagrinėjamo ginčo situacijoje svarbu yra tai, kad pati sukčiavimo ataka, kai sukčiai ragina spausti neva siuntų pristatymo ar kitos veiklos bendrovių nuorodas, turint tikslą už parduodamas prekes lėšas gauti į sąskaitą, yra plačiai žinoma visuomenėje, nes tiek bankai, tiek pačios bendrovės, tiek skelbimų portalai, tiek ir kitos institucijos viešai įvairiais vartotojams prieinamais kanalais skelbia informaciją apie šį sukčiavimo būdą ir ragina nespausti aktyvių nuorodų ir nesuvesti savo mokėjimo priemonės duomenų, norint lėšas gauti į savo sąskaitą.

Įvertinus pirmiau minėtą informaciją, nėra pagrindo teigti, kad, atsižvelgiant į sukčiavimo atakos pobūdį, pareiškėjas neturėjo galimybių kritiškai įvertinti trečiųjų asmenų jam atsiųstos žinutės su aktyvia nuoroda ir susilaikyti nuo tolimesnių veiksmų.

Vertinant tolesnius pareiškėjo veiksmus, paspaudus aktyvią nuorodą ir patekus į trečiųjų asmenų suklastotą banko puslapį, svarbu tai, kad pareiškėjas tikėjosi, kaip jis pats paaiškino, sumokėti už paslaugas 5 Eur, t. y. pareiškėjas nesiekė susieti Kortelės su *Apple Pay* naujame įrenginyje. Vis dėlto, ginčo byloje turimais duomenimis, pareiškėjas ne tik suvedė savo personalizuotus saugos duomenis, bet ir suvedė vienkartinį Kortelės pridėjimo prie *Apple Pay* kodą, taip patvirtindamas trečiųjų asmenų įrenginyje Kortelės pridėjimą prie *Apple Pay* sistemos bei Kortelės skaitmeninės versijos sukūrimą. Pareiškėjas nekomentuoja, kodėl pateikė šį kodą tretiesiems asmenims. Vis dėlto banko Lietuvos bankui pateikti duomenys įrodo, kad, prieš suvesdamas kodą, kad Kortelė būtų susieta su *Apple Pay*, pareiškėjas prisijungė prie savo interneto banko paskyros ir turėjo galimybę susipažinti su informacija apie kodo paskirtį[4].

Svarbu pažymėti, kad banko pranešimo teksto, kuriuo pareiškėjas buvo informuojamas apie pridėjimo prie *Apple Pay* sistemos kodą, turinys yra nedviprasmiškas ir informatyvus, t. y. aiškiai nurodomas konkretus veiksmas, kam skirtas kodas (pridėti Kortelę prie *Apple Pay* sistemos) ir kam jis neskirtas (mokėjimo patvirtinimas). Iš banko pareiškėjui pateiktos informacijos galima teigti, kad rūpestingas ir atidus vartotojas turėjo visas galimybes pamatyti informaciją apie veiksmą, kurį tvirtina suvesdamas kodą, ir susilaikyti nuo tolimesnių veiksmų. Vis dėlto surinkti duomenys leidžia daryti išvadą, kad pareiškėjas, prieš pateikdamas tretiesiems asmenims Kortelės prijungimo prie *Apple Pay* kodą, nekreipė deramo dėmesio į banko jam rodomą informaciją, ją dėl nežinomų priežasčių ignoravo.

Pareiškėjas, 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 nepaisydamas to, kokią informaciją bankas jam rodė.

Įvertinus pirmiau nurodytas aplinkybes, Lietuvos banko nuomone, galima daryti išvadą, kad pareiškėjas būtų galėjęs išvengti neautorizuotos ginčijamos mokėjimo operacijos iš savo sąskaitos įvykdymo, jeigu būtų buvęs pakankamai kritiškas savo su mokėjimo priemone atliekamų veiksmų atžvilgiu ir būtų susilaikęs nuo veiksmų su savo mokėjimo priemone. Pareiškėjas turėjo galimybę suprasti, kad jo prašoma atlikti veiksmus, kuriais tvirtinamas Kortelės prijungimas prie *Apple Pay* trečiųjų asmenų įrenginyje, nors pats pareiškėjas nurodė, kad tikėjosi tik sumokėti už paslaugą – atlikti 5 Eur mokėjimo operaciją. Pareiškėjas teigia supratęs, kad jo prašoma atlikti veiksmus, kuriais tvirtinamas mokėjimo operacijos įvykdymas, nors, kaip minėta, bankas prieš Kortelės susiejimą su *Apple Pay* pateikė pareiškėjui vienkartinį prijungimo kodą, nurodydamas, kad šis kodas skirtas ne mokėjimo operacijoms atlikti, o būtent Kortelei su *Apple Pay* susieti. Vis dėlto pareiškėjas į šią banko rodytą informaciją nekreipė dėmesio ir vykdė trečiųjų asmenų jam pateiktus nurodymus, tai ir lėmė, kad iš pareiškėjo banko sąskaitos buvo įvykdyta ginčijama mokėjimo operacija. Lietuvos banko vertinimu, toks pareiškėjo elgesys gali būti pripažintas kaip elgesys, iš esmės besiskiriantis nuo atsargaus elgesio reikalavimų, galiausiai ir lėmęs, kad tretieji asmenys įgijo galimybę pareiškėjo vardu inicijuoti mokėjimo operacijas.

Taigi, įvertinus ginčo byloje turimus duomenis ir ginčo šalių paaiškinimus apie ginčijamo mokėjimo 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.

---

[4] Pareiškėjui banko pateikta žinutė (jo pasirinkta kalba (angl.): *„Your security code for adding the card to Apple Pay is 486551. The code will be active for 30 minutes. Important! This code is not intended for payment confirmation. Enter the code only in the Apple Pay. Don't disclose this code to anyone.*"

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, jog buvo įvykdytas neautorizuotas ginčijamas mokėjimas 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 neautorizuoto ginčijamo mokėjimo lėšas yra nepagrįstas ir atmestinas.

2. Dėl banko sprendimo atmesti pareiškėjo prašymą pradėti lėšų grąžinimo procedūrą pagrįstumo

Kreipimesi į Lietuvos banką pareiškėjas taip pat nurodė, kad bankas turėjo inicijuoti lėšų grąžinimo procedūrą ir padėti pareiškėjui susigrąžinti lėšas.

Vertinant pareiškėjo keliamo reikalavimo pagrįstumą, svarbu pažymėti, kad papildomos galimybės kortelės turėtojui susigrąžinti pinigines lėšas tų mokėjimo operacijų, kurios yra tinkamai autorizuotos, nustatytos tarptautinės mokėjimo kortelių organizacijos *MasterCard* taisyklėse. Nei Lietuvos Respublikos teisės aktai, nei Europos Sąjungos teisės aktai nereglamentuoja, kokiomis sąlygomis turi būti vykdomos tokios lėšų grąžinimo procedūros. Taigi, banko veiksmai, ginčijant autorizuotas mokėjimo operacijas, reglamentuoti minėtose tarptautinės mokėjimo kortelių organizacijos *MasterCard* taisyklėse, kuriose nustatyti atvejai ir tvarka, pagal kuriuos bankas, gavęs kliento prašymą, gali kreiptis į tarptautinę mokėjimo kortelių organizaciją *MasterCard* dėl lėšų grąžinimo procedūros taikymo.

Vadovaujantis *MasterCard* taisyklėmis (33–35, 95 ir 96 psl.), operacijų mokėjimo kortele negalima ginčyti kaip atliktų neteisėtai, t. y. be kortelės turėtojo žinios (angl. *Fraud*), jeigu vartotojas dalyvauja mokėjimo operacijoje ir (ar) duoda leidimą atlikti mokėjimo operaciją. Bankas pažymi, kad ginčijamas mokėjimas buvo autentifikuotas, prie *Apple Pay* sistemos pridėjus mokėjimo kortelę. Taip pat iš banko pateiktų duomenų matyti, kad ginčijamas mokėjimas turėjo būti patvirtintas mobiliajame įrenginyje įdiegtu ir vartotojo pasirinktu saugumo nustatymo būdu[5]. Dėl šių priežasčių, vadovaujantis tarptautinės organizacijos *MasterCard* taisyklėmis, ginčyti jo kaip atlikto be pareiškėjo žinios bei prisidėjimo, bankas neturi galimybės.

Darytina išvada, kad bankas pagrįstai atsisakė pradėti lėšų grąžinimo procedūrą, o pareiškėjo argumentai, kad bankas nepagrįstai nedėjo pakankamai pastangų, kad lėšų grąžinimo procedūra būtų pradėta, yra atmestini kaip nepagrįsti objektyviais duomenimis.

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 argumentą[6].

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

---

[5] Iš banko pateiktų duomenų matyti, kad šiuos būdus nustato įmonė *Apple*, kuri ir teikia *Apple Pay* paslaugą, o ji numato, kad *Apple Pay* veikia su „Face ID“ arba „Touch-ID“, kad būtų užtikrinta dviejų lygių autentifikacija. Ši autentifikacija yra būtina tam, kad būtų patvirtintos mokėjimo operacijos.

[6] 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.

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