



**LIETUVOS BANKO  
TEISĖS IR LICENCIJAVIMO DEPARTAMENTO  
DIREKTORIUS**

**SPRENDIMAS  
DĖL X. X. IR REVOLUT BANK UAB GINČO NAGRINĖJIMO**

2023-03-22 Nr. 429-158  
Vilnius

Lietuvos bankas gavo *Refundee Ltd* (toliau – pareiškėjos atstovė), atstovaujančios X. X. (toliau – pareiškėja) interesams, kreipimąsi, kuriuo prašoma išnagrinėti tarp pareiškėjos ir *Revolut Bank UAB* (toliau – bankas) kilusį ginčą.

**N u s t a t y t a:**

2023 m. sausio 18 d. banko pareiškėjai išduota *VISA* mokėjimo kortele Nr. (*duomenys neskelbiami*) (toliau – Kortelė), panaudojant *Google Pay* mokėjimo metodą, įvykdytos trys mokėjimo operacijos, kurių suma 7 500 Eur (8 125,98 USD), gavėjui „Mne\*95017678as\_tech\_di“ (toliau – Operacijos).

Tą pačią dieną pareiškėja kreipėsi į banką ir nurodė, kad galimai tapo sukčių auka. Pareiškėja teigė, kad su ja telefonu susisiekė tariamas banko atstovas, kuriam pareiškėja pateikė visus savo duomenis. Pareiškėja pažymėjo, kad atskleidus duomenis iš karto buvo įvykdytos Operacijos. Dėl šios priežasties pareiškėja kreipėsi į banką ir prašė padėti susigrąžinti Operacijų metu prarastas lėšas.

Gavęs pareiškėjos kreipimąsi, bankas pradėjo vidinį tyrimą dėl galimo sukčiavimo. Įvertinęs pareiškėjos pateiktus duomenis, bankas pasiūlė pareiškėjai užpildyti prašymą dėl lėšų gražinimo procedūros (angl. *chargeback*) inicijavimo.

2023 m. sausio 18 d. pareiškėja pateikė lėšų gražinimo prašymą, tačiau bankas, įvertinęs visus surinktus duomenis, jį atmetė. Bankas tokį sprendimą priėmė, nes nustatė, kad nebuvo rasta jokių apgaulingos veiklos pareiškėjos atsiskaitomojoje sąskaitoje požymių, todėl už Operacijų atlikimą atsakinga turėtų būti būtent pati pareiškėja.

Gavusi banko sprendimą, pareiškėja 2023 m. sausio 19 d. kreipėsi į banką ir prašė sprendimą persvarstyti, tačiau bankas 2023 m. sausio 20 d. pareiškėjai pateikė atsakymą, kuriame nurodė, kad priimtas sprendimas yra pagrįstas ir nebus keičiamas. Pareiškėja su tuo nesutiko, todėl tarp šalių kilo ginčas.

Kreipimesi į Lietuvos banką pareiškėja prašo rekomenduoti bankui grąžinti Operacijų metu iš pareiškėjos atsiskaitomosios sąskaitos nurašytas lėšas. Pareiškėjos atstovė kreipimesi į Lietuvos banką pateikė tokius pat duomenis, kaip pirmajame kreipimesi į banką, t. y. kad pareiškėja tapo sukčių auka ir iš jos atsiskaitomosios sąskaitos buvo nurašytos lėšos. Pareiškėjos atstovė pažymėjo, kad pareiškėja neišreiškė savo valios atlikti Operacijų, todėl Operacijų metu pervestos lėšos turi būti grąžintos pareiškėjai, taip pat nurodė, kad tretieji asmenys telefoninio pokalbio metu, pasinaudodami tuo, kad pareiškėja prižiūrėjo ir maitino neseniai gimusį kūdikį, įtikino pareiškėją atskleisti visus personalizuotus saugumo duomenis. Pareiškėjos atstovė akcentavo, kad iš karto suvokusi, kad buvo atliktos Operacijos, pareiškėja užblokavo mokėjimo kortelę. Pareiškėjos atstovės teigimu, bankas turi prisiimti atsakomybę, nes Operacijos buvo autorizuotos mokėjimo kortele, kuri buvo naujai pridėta prie *Google Pay* paskyros. Pareiškėjos atstovė nurodė, kad tai bankui turėjo sukelti įtarimą, kad yra atliekama sukčiavimo ataka. Pareiškėjos atstovės nuomone, bankas privalėjo patikrinti atliekamas Operacijas ir jas blokuoti. Dėl šios priežasties pareiškėjos atstovė nurodo, kad nesutinka su banko priimtu sprendimu ir mano, kad bankas turėtų grąžinti iš pareiškėjos sąskaitos nepagrįstai nurašytas lėšas.

Atsiliepime į pareiškėjos kreipimąsi bankas nurodo nesutinkąs su pareiškėjos reikalavimu ir prašo jį atmesti. Banko teigimu, Operacijos buvo atliktos ir autorizuotos dviem mobiliaisiais

įrenginiais, kurių pavadinimai – „c2Ftc3VuZyAtIFNNLUE1MzZC“ ir „c2Ftc3VuZyAltFnnLUE1MjhC“. Banko teigimu, 2023 m. sausio 23 d. šie mobilieji įrenginiai, kaip *Google Pay* mokėjimo įrenginiai, buvo pridėti ir autorizuoti pačios pareiškėjos. Bankas nurodo, kad, norint pridėti mokėjimo kortelę prie įrenginio, kuriuo siekiama atlikti mokėjimo operacijas, kortelės turėtojas ar kita trečioji šalis turi ne tik įvesti mokėjimo kortelės duomenis (kortelės numerį, galiojimo datą ir kortelės saugos kodą CVV), bet tai padarius ir patvirtinti mokėjimo kortelę, įvedant vienkartinį saugos kodą, gautą trumpąja SMS žinute. Banko teigimu, žinutė su vienkartinio kodu visais atvejais yra siunčiama į telefono numerį, kuris buvo nurodytas ir autorizuotas vartotojo, kai buvo sudaroma sutartis su banku. Bankas nurodo, kad ir šiuo atveju apsaugos žinutės buvo išsiųstos pareiškėjos nurodytu numeriu, kurį pareiškėja patvirtino registruojant paskyrą ir sudarant sutartį su banku. Bankas akcentavo, kad toks saugumo kriterijus lemia tai, kad tretieji asmenys negalėtų pasinaudoti mokėjimo kortele ir be pareiškėjos žinios pridėti mokėjimo kortelės ir atlikti mokėjimo operacijų.

Banko teigimu, kartu su vienkartiniais saugos kodais pareiškėjai trumposiose SMS žinutėse buvo nurodyta šių kodų paskirtis bei perspėjimai šių kodų neperduoti tretiesiems asmenims, tačiau pareiškėja elgėsi nepakankamai apdairiai, nes atskleidė vienkartinius kodus tretiesiems asmenims. Bankas atkreipia dėmesį į tai, kad, nesuvedus vienkartinių saugos kodų į *Google Pay*, pareiškėjos mokėjimo kortelės pridėjimas nebūtų buvęs patvirtintas ir atsiskaitymai su *Google Pay* būtų buvę neįmanomi. Bankas nurodo neteigiantis, kad pareiškėja pati naudojo *Google Pay*, tačiau iš turimų sistemų duomenų akivaizdu, kad pareiškėjos mokėjimo priemonė prie *Google Pay* galėjo būti ir buvo pridėta pareiškėjai atskleidus tik jai žinomą informaciją (mokėjimo kortelės duomenis ir vienkartinius saugos kodus). Banko teigimu, pareiškėja pati tretiesiems asmenims atskleidė duomenis ir tokiais savo veiksmais patvirtino mokėjimo kortelės pridėjimą prie *Google Pay*, taigi, elgėsi aplaidžiai ir nerūpestingai, todėl bankui nekyla pareiga gražinti pareiškėjos prarastų lėšų. Bankas prašo atmesti pareiškėjos reikalavimą kaip nepagrįstą.

#### K o n s t a t u o j a m a :

Vadovaujantis Lietuvos banko valdybos 2012 m. sausio 26 d. nutarimu Nr. 03-23 patvirtintų Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių 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. Lietuvos bankas ginčo nagrinėjimo proceso metu neatlieka Lietuvos Respublikos Lietuvos banko įstatymo 42<sup>1</sup> straipsnyje reglamentuojamų patikrinimų, skirtų faktinėms aplinkybėms dėl Lietuvos banko prižiūrimo finansų rinkos dalyvio galimai padaryto Lietuvos banko kompetencijai priskirtų teisės aktų reikalavimų pažeidimo nustatyti ir įvertinti. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Pareiškėjos ir banko ginčas kilo dėl banko atsisakymo gražinti pareiškėjai jos mokėjimo kortelę, panaudojant *Google Pay* mokėjimo metodą, atliktų Operacijų, kurių atlikti pareiškėja teigia nedavusi sutikimo, sumą.

Pareiškėja neigia autorizavusi Operacijas ir (ar) pridėjusi savo mokėjimo kortelę prie *Google Pay* sistemos naujuose įrenginiuose bei tvirtina, kad lėšos iš jos atsiskaitomosios sąskaitos buvo nurašytos dėl to, kad tretieji asmenys galėjo pasisavinti pareiškėjos mokėjimo kortelės duomenis. Dėl šios priežasties pareiškėja prašo banko gražinti Operacijų metu tretiesiems asmenims pervestas lėšas. Atsiliepime bankas nurodo, kad Operacijos mokėjimo kortele įvykdytos ne dėl sutrikimų banko ar tarptautinės mokėjimo kortelių organizacijos *VISA* sistemoje ar saugumo spragų jose, o dėl pareiškėjos veiksmų, kuriais tretiesiems asmenims buvo atskleisti pareiškėjos mokėjimo priemonių personalizuoti saugumo duomenys ir dėl to tretieji asmenys įgijo galimybę savo įrenginiais inicijuoti Operacijas pareiškėjos atsiskaitomoje sąskaitoje.

Mokėjimo paslaugų teikėjų veiklą ir atsakomybę, mokėjimo paslaugas, jų teikimo sąlygas ir informavimą 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).

Bankas atsiliepime nurodo, kad pareiškėjos ginčijamos Operacijos buvo atliktos naudojantis trečiųjų asmenų įrenginiuose įdiegtu *Google Pay* mokėjimo įrenginiu, prie atitinkamų įrenginių, kuriuose veikia *Google Pay* sistema, pridėjus pareiškėjos mokėjimo kortelę. Taigi, šalių neginčijamomis aplinkybėmis, Operacijos buvo inicijuotos ir įvykdytos trečiųjų asmenų, jiems neteisėtu būdu sužinojus (pasisavinus) pareiškėjos mokėjimo priemonių personalizuotus saugumo duomenis ir juos panaudojus naujuose įrenginiuose pridėdant pareiškėjos mokėjimo kortelę prie *Google Pay* sistemos ir inicijuojant bei įvykdant Operacijas. Akivaizdu, kad Operacijų inicijavimas ir patvirtinimas neatitiko pačios pareiškėjos valios, nors formaliai (pagal išorinius požymius) ir sutapo su pareiškėjos ir banko sutarta sutikimo atlikti mokėjimo operacijas davimo forma ir tvarka.

Pareiškėjos nurodytos aplinkybės, kad Operacijos nėra pareiškėjos autorizuotos, o pareiškėjos mokėjimo kortelę prie *Google Pay* sistemos naujuose įrenginiuose pridėjo ne pareiškėja, o tretieji asmenys, bankas atsiliepime neginčija, todėl Lietuvos bankas daro išvadą, kad Operacijos, atliktos nesant pareiškėjos valios, jai net nežinant apie Operacijų inicijavimo aplinkybę bei neišreiškus jokių valinių veiksmų, kad Operacijos būtų patvirtintos, laikytinos neautorizuotomis.

Siekiant išspręsti tarp pareiškėjos ir banko kilusį ginčą bei pasisakyti dėl pareiškėjos keliamų reikalavimų pagrįstumo, Lietuvos banko vertinimu, būtina nustatyti, ar: 1) *dėl neautorizuotų Operacijų bankas privalo pareiškėjai kompensuoti jos patirtus nuostolius;* 2) *bankas turėjo galimybę ir pareigą atšaukti Operacijas;* 3) *banko teikiamos paslaugos buvo saugios.*

#### 1. *Dėl neautorizuotų Operacijų pasekmių ir pareiškėjos teisės į Operacijų sumos gražinimą*

Pagal Mokėjimų įstatymo 38 straipsnio 1 dalį, mokėtojo mokėjimo paslaugų teikėjas privalo gražinti mokėtojui neautorizuotos mokėjimo operacijos sumą ne vėliau kaip iki kitos darbo dienos nuo sužinojimo apie tokios mokėjimo operacijos įvykdymą, išskyrus atvejus, kai mokėtojo mokėjimo paslaugų teikėjas turi pagrįstų priežasčių įtartai mokėtojo sukčiavimą ir apie šias priežastis raštu praneša priežiūros institucijai (Lietuvos bankui).

Mokėjimų įstatymo 39 straipsnio 1 dalis nustato, kad mokėtojui gali tekti dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai iki 50 Eur, 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 1) jis iki mokėjimo operacijos įvykdymo negalėjo pastebėti mokėjimo priemonės praradimo, vagystės arba neteisėto pasisavinimo, išskyrus atvejus, kai jis veikė nesąžiningai; 2) nuostoliai yra patirti dėl mokėjimo paslaugų teikėjo, jo darbuotojo, tarpininko, filialo ar asmenų, kuriems perduotas veiklos funkcijų valdymas, veiksmų ar neveikimo.

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. Tokiais atvejais šio straipsnio 1 dalyje nustatytas didžiausias nuostolių sumos ribojimas netaikomas.“

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 (Mokėjimų įstatymo 34 straipsnio 2 dalis).

Mokėjimų įstatymas aiškiai nustato, kad tuo atveju, kai mokėtojas neigia autorizavęs įvykdytą mokėjimo operaciją, mokėtojo mokėjimo paslaugų teikėjo arba atitinkamais atvejais mokėjimo inicijavimo paslaugos teikėjo užregistruotas mokėjimo priemonės naudojimas nebūtinai yra pakankamas įrodymas, kad mokėtojas autorizavo mokėjimo operaciją ar veikė

nesąžiningai arba tyčia ar dėl didelio neatsargumo neįvykdė vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų. Mokėtojo mokėjimo paslaugų teikėjas ir atitinkamais atvejais mokėjimo inicijavimo paslaugos teikėjas turi pateikti įrodymų, kuriais patvirtinamas mokėtojo sukčiavimas arba didelis neatsargumas (Mokėjimų įstatymo 37 straipsnio 3 dalis).

Įvertinus pirmiau nurodytas Mokėjimų įstatymo nuostatas, galima teigti, kad mokėtojo mokėjimo paslaugų teikėjas gali būti visiškai atleistas nuo pareigos gražinti mokėtojui neautorizuotos mokėjimo operacijos sumą tik tuo atveju, jeigu pateikia įrodymų dėl mokėtojo sukčiavimo (nesąžiningumo arba tyčios) arba didelio neatsargumo (Mokėjimų įstatymo 37 straipsnio 3 dalis ir 39 straipsnio 3 dalis).

Aplinkybių ir duomenų, kaip ir šalių ginčo dėl to, kad pareiškėja galėjo veikti nesąžiningai arba tyčia, įskaitant sukčiavimą, nėra. Tai reiškia, kad, siekiant įvertinti, ar bankas pagrįstai atsisako kompensuoti pareiškėjos nuostolius, susijusius su Operacijų įvykdymu, ir ar galėtų pareiškėjos atžvilgiu būti taikoma Mokėjimų įstatymo 39 straipsnio 3 dalis, būtina nustatyti, ar pareiškėjos elgesys, atskleidžiant tam tikrus personalizuotus mokėjimo priemonės (banko išduotos mokėjimo kortelės) požymius, ir (ar) kiti veiksmai, dėl kurių galėjo būti įvykdytos Operacijos, vertintini kaip didelis pareiškėjos neatsargumas, dėl kurio visi jos reikalaujami atlyginti nuostoliai turėtų tekti pačiai pareiškėjai.

Antrosios mokėjimo paslaugų direktyvos (toliau – PSD2) preambulės 72 punkte rašoma, kad „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 ir 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>

Bankas mano, kad nuostolius dėl Operacijų pareiškėja patyrė dėl savo didelio neatsargumo, t. y. pareiškėja, perduodama tretiesiems asmenims savo mokėjimo kortelės duomenis (mokėjimo kortelėje nurodytus savo vardą, pavardę, kortelės numerį ir CVV kodą) bei vienkartinis banko pareiškėjai jos nurodytu telefono numeriu siųstus mokėjimo kortelės pridėjimo prie *Google Pay* sistemos saugos kodus, suteikė leidimą tretiesiems asmenims pridėti mokėjimo kortelę prie jų faktiškai valdomuose įrenginiuose įdiegto *Google Pay* atsiskaitymo įrenginio ir taip suteikė galimybę tretiesiems asmenims mokėjimo kortelės sąskaitoje vykdyti Operacijas pareiškėjos vardu.

Vertinamų aplinkybių kontekste visų pirma būtina pažymėti, kad, remiantis pirmiau minėtų Mokėjimų įstatymo nuostatų analize, mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai tik tuo atveju, jei tenkinamos abi sąlygos, t. y. mokėtojas ne tik neįvykdė vienos ar kelių jam Mokėjimų įstatyme nustatytų pareigų, bet ir padaro tai elgdamasis nesąžiningai arba tyčia, arba būdamas labai neatsargus.

Taigi, banko sprendimas nekompensuoti pareiškėjos nuostolių dėl neautorizuotų Operacijų įvykdymo galėtų būti vertinamas kaip pagrįstas tik tuo atveju, jei būtų įrodyta, kad pareiškėja, atskleisdama tam tikrus personalizuotus savo mokėjimo priemonių saugumo duomenis ir taip įgalindama trečiuosius asmenis panaudoti šiuos duomenis pareiškėjos mokėjimo kortelei prie *Google Pay* sistemos naujuose mobiliuosiuose įrenginiuose pridėti, o vėliau ir inicijuoti Operacijas, elgėsi itin aplaidžiai – buvo labai neatsargi.

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 privatiems klientams taikomų mokėjimo paslaugų teikimo sąlygų (toliau – Sąlygos) 9 punkte nustatyta, kad „darome viską, ką galime, kad apsaugotume jūsų pinigus. To paties prašome ir jūsų – saugoti savo saugumo informaciją ir „Revolut“ kortelę. Tai reiškia, jog neturėtumėte savo saugumo informacijos laikyti šalia „Revolut“ kortelės ir turėtumėte juos paslėpti arba apsaugoti, jei kur nors užsirašote ar laikote. Savo saugumo informacijos nepateikite niekam kitam.“<sup>2</sup>

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

<sup>2</sup> <https://www.revolut.com/lt-LT/legal/terms/>

Taigi, pirmiau aptartos Sąlygų nuostatos aiškiai nustato, kad už mokėjimo ir tapatybės patvirtinimo priemonių personalizuotų saugumo duomenų konfidencialumą yra atsakingas mokėtojas, šiuo atveju – pareiškėja, ji privalo užtikrinti, kad minėti duomenys netaptų žinomi tretiesiems asmenims. Atsižvelgiant į tai, manytina, kad pareiškėjos elgesys būtų laikomas kaip atitinkantis mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, jei būtų nustatyta, kad pareiškėja ėmėsi adekvačių veiksmų (ar priešingai – nustačius, kad nuo tam tikrų veiksmų susilaikė) tam, kad jai banko išduotų mokėjimo priemonių personalizuotų saugumo duomenų, įgalinančių inicijuoti ir tvirtinti mokėjimus, konfidencialumas būtų tinkamai užtikrintas.

Lietuvos bankas, įvertinęs pareiškėjos kreipimesi ir banko atsiliepime nurodytas aplinkybes bei kartu su kreipimusi ir atsiliepimu pateiktus duomenis, nustatė, kad su pareiškėja prieš Operaciją įvykdymą susiekė tretieji asmenys, kurie prisistatė banko darbuotojais. Tretieji asmenys įtikino pareiškėją, kad jos atsiskaitomojoje sąskaitoje yra atliekama neteisėta veikla, t. y. sukčiai Didžiojoje Britanijoje bando pasisavinti pareiškėjos atsiskaitomojoje sąskaitoje esančias lėšas. Tam, kad būtų apsaugotos pareiškėjos lėšos, tretieji asmenys prašė pateikti duomenis ir atlikti tam tikrus veiksmus. Iš pateiktų duomenų (pirminių pareiškėjos paaiškinimų bankui) matyti, kad pareiškėja telefoninio pokalbio metu pateikė visus trečiųjų asmenų prašomus duomenis, t. y. mokėjimo kortelės duomenis ir pareiškėjai atsiųstus vienkartinis saugos kodus, nes dar tebesitęsiant pokalbiui telefonu buvo atliktos Operacijos, kurių metu buvo pasisavintos pareiškėjos lėšos.

Bankas kartu su atsiliepimu Lietuvos bankui pateikė vidinės sistemos duomenis, kurie patvirtina, kad pareiškėjos ginčijamos Operacijos mokėjimo kortele buvo inicijuotos pasinaudojant *Google Pay* mokėjimo metodu. Remiantis atsiliepime teikiamais paaiškinimais, tam, kad būtų galima atsiskaityti pasinaudojant *Google Pay* mokėjimo metodu, visų pirma būtina mokėjimo kortelę pridėti prie *Google Pay* sistemos. Mokėjimo kortelei prie *Google Pay* sistemos pridėti yra taikoma saugesnio autentiškumo patvirtinimo procedūra, kurios metu reikia ne tik pateikti mokėjimo kortelės duomenis, bet ir suvesti vienkartinį saugos kodą, tai, remiantis banko pateiktais įrodymais, ir buvo atlikta. Aplinkybę, kad tretieji asmenys, tikindami, kad siekia apsaugoti pareiškėjos sąskaitoje esančias lėšas, prašė pateikti tiek mokėjimo kortelės duomenis, tiek į telefoną atsiųstus vienkartinis saugos kodus, pripažįsta ir pati pareiškėja. Šiuos duomenis patvirtina tiek pareiškėjos bankui pateikti duomenys, tiek pareiškėjos kreipimesi į Lietuvos banką pateikta informacija.

Vadinasi, ginčo byloje esančiais duomenimis, pareiškėjos mokėjimo kortelė prie *Google Pay* sistemos naujuose įrenginiuose buvo pridėta, suvedus pareiškėjos mokėjimo kortelės personalizuotus saugumo duomenis, taip pat būtent į pareiškėjos mobilųjį telefoną siųstus vienkartinis saugos kodus. Kaip minėta pirmiau, pareiškėja neginčija fakto, kad šiuos duomenis tretiesiems asmenims atskleidė, todėl tretieji asmenys dėl pareiškėjos aktyvių veiksmų sužinojo tik pareiškėjai žinomus personalizuotus saugumo duomenis, nes be vienkartinis saugos kodų objektyviai nebuvo galima pridėti mokėjimo kortelės prie *Google Pay* įrenginio ir atsiskaityti šiuo metodu.

Dėl šios priežasties pareiškėja, galimai nesuprasdama atliekamų veiksmų reikšmės bei pasekmių, atskleidė tretiesiems asmenims visus duomenis, būtinus jos mokėjimo kortelei pridėti prie *Google Pay* sistemos naujuose įrenginiuose, iš kurių vėliau ir inicijuotos pareiškėjos neautorizuotos Operacijos. Pareiškėjai perdavus tretiesiems asmenims SMS žinutėse jos telefono numeriu atsiųstus saugos kodus, mokėjimo kortelės pridėjimas naujuose įrenginiuose buvo patvirtintas, o atsiskaitymo *Google Pay* paslauga aktyvuota – ja naudojantis ir inicijuotos bei patvirtintos Operacijos, kurių suma pareiškėjai nėra iki šiol grąžinta.

Kaip nurodoma atsiliepime, nesuvedus pareiškėjos telefono numeriu išsiųstų vienkartinis saugos kodų į *Google Pay* sistemą, pareiškėjos mokėjimo kortelės pridėjimas nebūtų buvęs patvirtintas ir atsiskaitymai naudojantis *Google Pay* metodu būtų buvę neįmanomi: įvedus neteisingus saugos kodus, visas procesas yra pradedamas iš naujo, t. y. vėl prašoma suvesti mokėjimo kortelės duomenis, ši informacija perduodama mokėjimo paslaugų teikėjui, ją patvirtinus yra išsiunčiami nauji vienkartiniai saugos kodai SMS žinute.

Be to, bankas pateikė duomenis, kad, siunčiant vienkartinis saugos kodus, pareiškėjai SMS žinutėje papildomai buvo nurodyta šių kodų paskirtis bei perspėjimas šių kodų neperduoti tretiesiems asmenims, net jeigu šie asmenys ir tvirtina esantys banko darbuotojai<sup>3</sup>. Šios

<sup>3</sup> SMS žinutės tekstas anglų kalba: „This code will be used to add your card to another Google Pay device. Don` t share this code with anyone, even if they claim to be Revolut. Don` t enter it anywhere unless you want to add your card to a new device. Revolut verification code for Google Pay: \*\*\*\*\*.“

aplinkybės patvirtina, kad bankas, siekdamas užtikrinti, kad pareiškėja tinkamai įvertintų vienkartinį saugos kodą paskirtį ir neperduotų jį tretiesiems asmenims, informavo apie tai pareiškėja, tačiau pareiškėja nekreipė dėmesio į SMS žinučių turinį ir perdavė tretiesiems asmenims tik jai vienai siųstus ir žinomus vienkartinį saugos kodą.

Atkreiptinas dėmesys ir į tai, kad nebuvo nustatyta duomenų, kurių pagrindu būtų galima įžvelgti įsilaužimo į pareiškėjos sąskaitą, pareiškėjos duomenų atskleidimo, banko sistemų trikdžių ar neveikimo požymių.

Išanalizavęs šias bei visas kitas nustatytas aplinkybes ir ginčo byloje esančius duomenis, Lietuvos bankas daro išvadą, kad vis dėlto vertinti pareiškėjos elgesio kaip atsargaus ir apdairaus ar tik neatsargaus šiuo atveju nėra galima.

Kaip matyti iš nustatytų aplinkybių, Operacijas tretieji asmenys be pareiškėjos žinios galėjo atlikti tik dėl to, kad pareiškėja, būdama labai neatsargi, netinkamai įvykdė Mokėjimų įstatyme (34 straipsnis) ir su banku sudarytoje sutartyje įtvirtintus mokėjimo kortelės saugaus naudojimo reikalavimus. Nurodytos aplinkybės leidžia teigti, kad pareiškėja būtent dėl savo didelio neatsargumo neišsaugojo jos vardu išduotos mokėjimo kortelės duomenų konfidencialumo – nesiėmė tų saugumo priemonių, kurių privalėjo imtis, kad būtų tinkamai apsaugoti jai suteiktos mokėjimo priemonės duomenys, ir tretiesiems asmenims suteikė vienkartinį saugos kodą, kuriuos gavo į sau priklausantį telefono numerį trumpąją SMS žinute.

Konstatavus, kad pareiškėja, nesilaikydama jai, kaip mokėtojai, Mokėjimų įstatyme ir sutartyje su banku nustatytų pareigų, susijusių su išduotomis mokėjimo priemonėmis, elgėsi labai neatsargiai, kartu darytina išvada, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, nustatančią, kad tokiu atveju mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai. Dėl šios priežasties, Lietuvos banko vertinimu, bankas neturi pareigos grąžinti (kompensuoti) pareiškėjai neautorizuotos Operacijos lėšų.

## *2. Dėl galimybės atšaukti Operacijas*

Pareiškėjos atstovės kreipimesi teigiama, kad pareiškėja, supratusi, jog tapo sukčių auka, iškart ėmėsi priemonių tam, kad atšauktų Operacijas, t. y., naudodamasi banko mobiliąja programėle, susisiekė su banku, informavo apie ginčijamas Operacijas ir užpildė banko nurodytą prašymą dėl lėšų grąžinimo procedūros inicijavimo.

Vertinant pareiškėjos atstovės teiginius dėl Operacijų atšaukimo ir jų sumos grąžinimo į pareiškėjos sąskaitą banke, pažymėtina, kad, vadovaujantis Mokėjimų įstatymo 44 straipsnio 1 dalimi, 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).

Sąlygų 18 punkte yra numatyta, kad „mokėjimą (įskaitant periodinį mokėjimą arba SEPA tiesioginį debetą) galite atšaukti bet kuriuo metu iki darbo dienos, kuri yra prieš mokėjimo iš jūsų sąskaitos įvykdymo terminą, pabaigos. Negalite atšaukti mokėjimo tą pačią dieną, kai jis turi būti įvykdytas iš jūsų sąskaitos.“

Iš pareiškėjos ir banko pateiktų paaiškinimų matyti, kad pareiškėja dėl atliktų ginčijamų Operacijų kreipėsi jau po to, kai Operacijos buvo tinkamai autorizuotos šalių sudarytoje sutartyje sutarta forma ir tvarka ir negalėjo būti atšauktos po to, kai jas gavo pareiškėjos mokėjimo paslaugų teikėjas, šiuo atveju – bankas, todėl bankas, remiantis pirmiau minėtomis Mokėjimų įstatymo ir Sąlygų nuostatomis, neturėjo pareigos įvykdyti pareiškėjos prašymų atšaukti Operacijas, praėjus įstatyme nustatytam jo atšaukimo terminui ir (ar) grąžinti į pareiškėjos sąskaitą šios mokėjimo sumos.

## *3. Dėl banko teikiamų mokėjimo paslaugų saugumo*

Pareiškėjos atstovė, grįsdama bankui keliamą reikalavimą dėl nuostolių, susijusių su Operacijų įvykdymu, kompensavimo, nurodo ir tai, kad bankas nepagrįstai nepatikrino Operacijų ir jų neblokavo.

Pateiktuose paaiškinimuose dėl pirmiau minėtų pareiškėjos atstovės teiginių bankas nurodė, kad Operacijos buvo patvirtintos, todėl bankas pagal teisės aktų nuostatas privalėjo jas tinkamai įvykdyti. Bankas paaiškino, kad, atliekant mokėjimus nuotoliniu būdu, paslaugų (prekių) tiekėjai, kurių naudai šiuo atveju buvo atliktos Operacijos, nėra laikomi rizikingų šalių paslaugų (prekių) tiekėjais. Taip pat bankas pažymėjo, kad teisės aktai nenumato pareigos tikrinti mokėtojo pateiktų duomenų apie lėšų gavėją. Bankas nurodė, kad pareiškėja banko paslaugomis naudojasi nuo 2020 m. ir per tą laiką yra atlikusi ne vieną mokėjimą EUR ir USD valiuta įvairiomis sumomis ir dažnumu. Dėl šios priežasties banko saugumo sistema neužfiksavo Operacijų kaip įtartinų.

Kaip minėta, Lietuvos bankas nagrinėdamas ginčus neatlieka patikrinimų tam, kad nustatytų, ar nebuvo pažeisti finansų įstaigų veiklai keliami teisės aktų reikalavimai. Lietuvos bankas remiasi ginčo šalių pateiktais konkrečiais įrodymais, kurių pagrindu priima sprendimą. Atsižvelgiant į tai ir įvertinus byloje esančius bei pirmiau aptartus duomenis, būtina konstatuoti, kad nagrinėjant ginčą nebuvo nustatyta aplinkybių, galinčių patvirtinti pareiškėjos teiginį, kad bankas nesiėmė reikiamų veiksmų tam, kad apsaugotų pareiškėjos banko sąskaitose esančias lėšas ar kad banko teikiamos paslaugos yra nesaugios, o įvykdydamas Operacijas bankas būtų pažeidęs finansų rinką reglamentuojančių teisės aktų reikalavimus. Bankas teigia, kad atlikdamas pareiškėjos ginčijamas Operacijas vykdė mokėjimo operacijų stebėseną, tačiau šios Operacijos dėl pirmiau aptartų aplinkybių įtarimų nesukėlė, todėl nebuvo poreikio jų stabdyti.

Pažymėtina, kad vien aplinkybė, jog Operacijos, kurių atlikti sutikimo pareiškėja nurodo nedavusi, buvo įvykdytos, savaime nepagrindžia aplinkybės, kad banko taikytos saugumo priemonės šiuo konkrečiu atveju buvo ne tik nepakankamos, bet ir neatitinkančios teisės aktų reikalavimų, ir kad tai galėjo nulėmti Operacijų įvykdymą ir dėl to galėtų kilti banko civilinė atsakomybė Operacijų nulėmtus nuostolius pareiškėjai kompensuoti. Kaip minėta, duomenų, kad bankas būtų nevykdęs finansų rinką reglamentuojančių teisės aktų reikalavimų, nenustatyta.

Pareiškėjos atstovė savo deklaratyvių teiginių, kad banko teikiamos paslaugos yra nesaugios, o taikytos priemonės ir veiksmai buvo nepakankami tam, kad apsaugotų pareiškėjos mokėjimo kortelės sąskaitoje esančias lėšas, jokiais duomenimis nepagrindė. Priešingai, įvertinus ginčo byloje esančius įrodymus, padaryta išvada, kad pareiškėjos nuostolius dėl Operacijų įvykdymo nulėmė būtent pačios pareiškėjos itin neatsargūs veiksmais, atskleidžiant savo mokėjimo priemonių personalizuotus saugumo duomenis.

Taigi, įvertinus visa tai, kas išdėstyta pirmiau, ir nustačius, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, darytina išvada, kad pareiškėjos bankui keliamas reikalavimas gražinti ir (ar) kompensuoti Operacijų sumą yra nepagrįstas, todėl atmestinas.

Remdamasis tuo, kas išdėstyta, ir vadovaudamasis Lietuvos Respublikos vartotojų teisių apsaugos įstatymo 27 straipsnio 1 dalies 3 punktu, Lietuvos banko valdybos 2012 m. sausio 26 d. nutarimo Nr. 03-23 „Dėl Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių patvirtinimo“ 2 punktu ir šiuo nutarimu patvirtintų Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių 59.3 papunkčiu, n u s p r e n d ž i u:

Atmesti pareiškėjos X. X. reikalavimą.

Lietuvos banko sprendimas dėl ginčo esmės yra rekomendacinio pobūdžio ir teismui neskundžiamas. Vartotojui ir finansų rinkos dalyviui išlieka teisė dėl ginčo sprendimo kreiptis į teismą arba kitą ginčų nagrinėjimo instituciją 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.