LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

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

2022-12-07 Nr. 429-619
Vilnius

Lietuvos bankas gavo X. X. (toliau – pareiškėja) kreipimąsi, kuriuo prašoma išnagrinėti tarp pareiškėjos ir *Revolut Bank UAB (*buvusi *Revolut Payments UAB)*[1] (toliau – bankas) kilusį ginčą.

N u s t a t y t a:

2022 m. rugsėjo 28 d. banko pareiškėjai išduota *VISA* mokėjimo kortele Nr. (*duomenys neskelbiami*) (toliau – Kortelė), panaudojant *Apple Pay* mokėjimo metodą, įvykdyta mokėjimo operacija, kurios suma 9330 GBP (10 822,75 Eur), gavėjui „Selfridges" (toliau – Operacija).

Tą pačią dieną pareiškėja kreipėsi į banką ir nurodė, kad galimai tapo sukčių auka. Pareiškėja teigė, kad su ja telefonu susisiekė tariamas banko atstovas ir nurodė, kad bus reikalinga atlikti pareiškėjos mokėjimo sąskaitos saugumo patikrą, nes buvo identifikuota galimai neteisėta veikla. Pareiškėja pažymėjo, kad praėjus keletui valandų po pokalbio buvo įvykdyta Operacija, todėl pareiškėja išreiškė prašymą ją sustabdyti. Pareiškėja taip pat pažymėjo, kad ji nesuprato, jog jai skambinęs trečiasis asmuo yra sukčius, nes jis jai nurodė tikslius pareiškėjos kontaktinius duomenis, t. y. gyvenamosios vietos adresą ir telefono numerius. Pareiškėja pažymėjo, kad ji pateikė trečiajam asmeniui visus duomenis, išskyrus mokėjimo kortelės duomenis. Pareiškėja taip pat nurodo, kad pokalbio metu ji gavo atitinkamo turinio trumpąsias SMS žinutes bei elektroninius laiškus.

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

2022 m. rugsėjo 28 d. pareiškėja pateikė lėšų grąžinimo prašymą, tačiau bankas, įvertinęs visus surinktus duomenis, jį atmetė. Bankas tokį sprendimą priėmė, nes nustatė, kad nebuvo rasta jokių apgaulingos veiklos pareiškėjos atsiskaitomoje sąskaitoje požymių, todėl už Operacijos mokėjimo atlikimą atsakinga turėtų būti būtent pati pareiškėja.

Po priimto sprendimo pareiškėja 2022 m. spalio 5 d. kreipėsi į banką ir prašė jį peržiūrėti. Tačiau bankas 2022 m. spalio 12 d. pareiškėjai pateikė atsakymą, kuriame nurodė, kad priimtas sprendimas yra pagrįstas ir jis keičiamas nebus. Pareiškėja su tuo nesutiko, todėl tarp šalių kilo ginčas.

Kreipimesi į Lietuvos banką pareiškėja prašo rekomenduoti bankui grąžinti Operacijos metu iš pareiškėjos atsiskaitomosios sąskaitos nurašytas lėšas, t. y. grąžinti 9330 GBP. Pareiškėja kreipimesi į Lietuvos banką pateikė tokius pat duomenis, kaip ir pirminio kreipimosi metu į banką, t. y. kad pareiškėja tapo sukčių auka ir iš jos atsiskaitomosios sąskaitos buvo nurašytos lėšos. Pareiškėja nurodė, kad ji Operacijų neatliko, nes Operacijos buvo atliktos Londone, o ji tuo metu buvo *(duomenys neskelbiami)* mieste. Taip pat pareiškėja pažymi, kad mokėjimo operacijos buvo atliktos naudojant *Apple Pay* mokėjimo metodą, tačiau pareiškėja nei *Iphone* telefono, nei *Apple Pay* neturi. Pareiškėja nurodo, kad tuo metu, kai buvo atliktos mokėjimo operacijos, ji buvo darbe, todėl vietoje, kurioje jos mokėjimo kortele buvo įsigytos paslaugos, jos taip pat nebuvo. Dėl šios priežasties, pareiškėja nurodo, kad ji nesutinka su

[1] *Revolut Payments UAB* buvo reorganizuota, ją prijungiant prie *Revolut Bank UAB*, todėl nuo 2022 m. liepos 1 d. *Revolut Payments UAB* teisės ir pareigos pagal jos sudarytas galiojančias finansinių paslaugų ir kitas sutartis, įskaitant iš šių sutarčių kilusius ginčus, perėjo *Revolut Bank UAB*.

banko priimtu sprendimu ir mano, kad bankas turėtų grąžinti iš jos sąskaitos nepagrįstai nurašytas lėšas.

Atsiliepime į pareiškėjos kreipimąsi bankas nurodo nesutinkąs su pareiškėjos reikalavimu ir prašo jį atmesti. Banko teigimu, Operacija buvo atlikta mobiliuoju įrenginiu, kurio pavadinimas – „RGFuaWkncyBpUGhvbmU". Banko teigimu, 2022 m. rugsėjo 28 d. šis mobilusis įrenginys, kaip *Apple pay* mokėjimo įrenginys, buvo pridėtas ir autorizuotas pačios pareiškėjos. Bankas nurodo, kad norinti 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 vienkartiniu kodu visais atvejai yra siunčiama į telefono numerį, kuris buvo nurodytas ir autorizuotas vartotojo, kai buvo sudaroma sutartis su banku. Bankas nurodo, kad ir šiuo atveju apsaugos žinutė buvo išsiųsta 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 prisidėti mokėjimo kortelę ir atlikti mokėjimo operacijų.

Bankas taip pat pažymi ir tai, kad nors pareiškėja nurodo, kad tretiesiems asmenims nesuteikė unikalių mokėjimo kortelės saugos duomenų, tačiau toks pareiškėjos teiginys prieštarauja tam, kas pateikta aukščiau, nes norint pridėti mokėjimo kortelę prie *Apple Pay*, pareiškėja turėjo atskleisti mokėjimo kortelės duomenis ir į jos telefoną atsiųstą vienkartinį saugos kodą.

Bankas nurodo ir tai, kad kartu su vienkartiniu saugos kodu pareiškėjai trumpojoje SMS žinutėje buvo nurodyta šio kodo paskirtis bei perspėjimas šio kodo neperduoti tretiesiems asmenims. Tačiau pareiškėja elgėsi nepakankamai apdairiai, nes turėjo atskleisti vienkartinį kodą tretiesiems asmenims. Bankas atkreipia dėmesį į tai, kad be vienkartinio saugos kodo suvedimo į *Apple Pay*, pareiškėjos mokėjimo kortelės pridėjimas nebūtų buvęs patvirtintas ir atskaitymas su *Apple Pay* būtų buvęs neįmanomas. Bankas nurodo, kad jis neteigia, jog pareiškėja pati naudojosi Apple Pay, tačiau pagal turimus sistemų duomenis, akivaizdu, kad pareiškėjos mokėjimo priemonė prie Apple Pay galėjo būti ir buvo pridėta tik pareiškėjai atskleidus tik jai žinomą informaciją (mokėjimo kortelės duomenis ir vienkartinį saugos kodą). Taigi, bankas teigia, kadangi pareiškėja pati tretiesiems asmenims atskleidė duomenis ir tokiais savo veiksmais patvirtino mokėjimo kortelės pridėjimą prie Apple Pay, todėl tokiu būdu elgėsi aplaidžiai ir nerūpestingai, o bankui nekyla pareiga grąžinti 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. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Pareiškėjos ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjai jos mokėjimo kortele, panaudojant *Apple Pay* mokėjimo metodą, atliktos Operacijos, kurios vertė 9330 GBP, ir kurios atlikti pareiškėja teigia nedavusi sutikimo, sumą.

Pareiškėja neigia autorizavusi Operaciją ir (ar) pridėjusi savo mokėjimo kortelę prie *Apple Pay* sistemos naujame įrenginyje, 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 grąžinti Operacijos metu tretiesiems asmenims pervestas lėšas. Atsiliepime bankas nurodo, kad Operacija mokėjimo kortele įvyko 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, dėl ko tretieji asmenys įgijo galimybę savo įrenginiu inicijuoti Operaciją pareiškėjos atsiskaitomoje sąskaitoje.

Mokėjimo paslaugų teikėjų veiklą ir atsakomybę, mokėjimo paslaugas, jų teikimo sąlygas ir informavimo apie šias sąlygas reikalavimus, mokėjimo operacijų autorizavimą ir vykdymą, mokėjimo paslaugų vartotojų ir mokėjimo paslaugų teikėjų teises ir pareigas,

susijusias su mokėjimo paslaugomis, kai mokėjimo paslaugų teikimas yra verslas, reglamentuoja Lietuvos Respublikos mokėjimų įstatymas.

Mokėjimų įstatymo 29 straipsnio 1 dalyje nustatyta, kad mokėjimo operacija laikoma autorizuota tik tada, kai mokėtojas duoda sutikimą įvykdyti mokėjimo operaciją. Jeigu mokėtojo sutikimo įvykdyti mokėjimo operaciją nėra, laikoma, kad mokėjimo operacija yra neautorizuota (Mokėjimų įstatymo 29 straipsnio 2 dalis).

Bankas atsiliepime nurodo, kad pareiškėjos ginčijama Operacija buvo atlikta naudojantis trečiųjų asmenų įrenginyje įdiegtu *Apple Pay* mokėjimo būdu, prie atitinkamo įrenginio, kuriame veikia *Apple Pay* sistema, pridėjus pareiškėjos mokėjimo kortelę. Taigi, šalių neginčijamomis aplinkybėmis, Operacija buvo inicijuota ir įvykdyta trečiųjų asmenų, jiems neteisėtu būdu sužinojus (pasisavinus) pareiškėjos mokėjimo priemonių personalizuotus saugumo duomenis ir juos panaudojus naujame įrenginyje pridėti pareiškėjos mokėjimo kortelę prie *Apple Pay* sistemos, kuria pasinaudojant vėliau inicijuota ir įvykdyta pati Operacija. Akivaizdu, kad Operacijos inicijavimas ir patvirtinimas neatitiko pačios pareiškėjos valios, nors formaliai (išoriniais požymiais) ir sutapo su pareiškėjos ir banko sutarta sutikimo mokėjimo operacijoms davimo forma ir tvarka.

Pareiškėjos nurodytos aplinkybės, kad Operacija nėra pareiškėjos autorizuota, o pareiškėjos mokėjimo kortelė prie *Apple Pay* sistemos naujame įrenginyje pridėjo ne pareiškėja, o tretieji asmenys, bankas atsiliepime neginčija, todėl šio ginčo nagrinėjimo metu Lietuvos bankas daro išvadą, kad Operacija, atlikta nesant pareiškėjos valios ir jai net nežinant apie Operacijos inicijavimo aplinkybę bei neišreiškus jokių valinių veiksmų Operacijai patvirtinti, laikytina neautorizuota.

Siekiant išspręsti tarp pareiškėjos ir banko kilusį ginčą bei pasisakyti dėl pareiškėjos keliamų reikalavimų pagrįstumo, Lietuvos banko vertinimu, būtina nustatyti ar: 1) *dėl neautorizuotos Operacijos bankas privalo pareiškėjai kompensuoti jos patirtus nuostolius*; 2) *bankas turėjo galimybę ir pareigą atšaukti Operaciją*.

1. Dėl neautorizuotos Operacijos pasekmių ir pareiškėjos teisės į Operacijos sumos grąžinimą

Pagal Mokėjimų įstatymo 38 straipsnio 1 dalį, mokėtojo mokėjimo paslaugų teikėjas privalo grąžinti 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 įtarti 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 didžiausios 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 grąžinti 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 Operacijos 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 įvykdyta Operacija, 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."[2]

Bankas mano, kad nuostolius dėl Operacijos 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 vienkartinį banko pareiškėjai jos nurodytu telefono numeriu siųstą mokėjimo kortelės pridėjimo prie *Apply Pay* sistemos saugos kodą, suteikė leidimą tretiesiems asmenims pridėti mokėjimo kortelę prie jų faktiškai valdomame įrenginyje įdiegto *Apple Pay* atsiskaitymo būdo ir tokiu būdu suteikė galimybę tretiesiems asmenims mokėjimo kortelės sąskaitoje vykdyti Operaciją 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 neįvykdo vienos ar kelių jam Mokėjimų įstatyme nustatytų pareigų, bet ir padaro tai elgdamasis nesąžiningai arba tyčia, ar būdamas labai neatsargus.

Taigi, banko sprendimas nekompensuoti pareiškėjos nuostolių dėl neautorizuotos Operacijos įvykdymo galėtų būti vertinamas kaip pagrįstas tik tuo atveju, jei būtų įrodyta, kad pareiškėja, atskleisdama tam tikrus personalizuotus savo mokėjimo priemonių saugumo duomenis ir tokiu būdu įgalindama trečiuosius asmenis panaudoti šiuos duomenis pareiškėjos mokėjimo kortelei prie *Apple Pay* sistemos naujame mobiliajame įrenginyje pridėti, o vėliau ir inicijuoti Operaciją, 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

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

paslėpti arba apsaugoti, jei kur nors užsirašote ar laikote. Savo saugumo informacijos nepateikite niekam kitam[3]“.

Taigi, pirmiau aptartos Sąlygų nuostatos aiškiai nustato, kad už mokėjimo ir tapatybės patvirtinimo priemonių personalizuotų saugumo duomenų konfidencialumą yra atsakingas mokėtojas, šiuo atveju – pareiškėja, kuri 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 Operacijos įvykdymą susiekė tretieji asmenys, kurie prisistatė banko darbuotojais. Tretieji asmenys įtikino pareiškėją, kad jos atsiskaitomojoje sąskaitoje yra atliekama neteisėta veikla, todėl neva užblokavo pareiškėjos mokėjimo kortelę. Tam, kad atblokuoti pareiškėjos mokėjimo kortelę tretieji asmenys prašė pateikti duomenis ir atlikti tam tikrus veiksmus. Iš pateiktų duomenų matyti, kad pareiškėja turėjo pateikti trečiųjų asmenų prašomus duomenis, t. y. mokėjimo kortelės duomenis ir pareiškėjai atsiųstą vienkartinį saugos kodą, nes po dviejų valandų buvo atlikta Operacija, kurios metu buvo pasisavintos pareiškėjos lėšos.

Bankas kartu su atsiliepimu Lietuvos bankui pateikė vidinės sistemos duomenis, kurie patvirtina, kad pareiškėjos ginčijama Operacija mokėjimo kortele buvo inicijuota pasinaudojant *Apple Pay* mokėjimo metodu. Remiantis atsiliepime teikiamais paaiškinimais, tam, kad būtų galima atsiskaityti pasinaudojant *Apple Pay* mokėjimo metodu, visų pirma, būtina mokėjimo kortelę pridėti prie *Apple Pay* sistemos. Mokėjimo kortelei prie *Apple Pay* sistemos pridėti yra taikoma saugesnio autentiškumo patvirtinimo procedūra, kurios metu reikia ne tik pateikti mokėjimo kortelės duomenis, bet ir suvesti vienkartinį saugos kodą, kas, pagal banko pateiktus įrodymus, ir buvo atlikta šiuo atveju. Aplinkybę, kad tretieji asmenys, įtikindami, kad siekia atblokuoti jos mokėjimo kortelę, prašė pateikti tiek mokėjimo kortelės duomenis, tiek ir į jos telefoną atsiųstą vienkartinį saugos kodą, pripažįsta ir pati pareiškėja. Šiuos duomenis patvirtina tiek pareiškėjos bankui pateikti duomenys, tiek pareiškėjos kreipimesi į Lietuvos banką pateikta informacija.

Įrodymų pakankamumo taisyklė civiliniame procese grindžiama vadinamąja tikėtinumo taisykle (tikimybių pusiausvyros principu). Kasacinio teismo jurisprudencijoje ne kartą pažymėta, kad įrodinėjimas civiliniame procese turi savo specifiką – nenustatyta, kad išvadą apie tam tikrų faktų buvimą galima daryti tik tada, kai dėl jų egzistavimo absoliučiai nėra abejonių; išvadą apie faktų buvimą teismas civiliniame procese gali daryti ir tada, kai tam tikros abejonės dėl fakto buvimo išlieka, tačiau byloje esančių įrodymų visuma leidžia manyti esant labiau tikėtina atitinkamą faktą buvus, nei jo nebuvus[4].

Vadinasi, ginčo byloje esančiais duomenimis, pareiškėjos mokėjimo kortelė prie *Apple Pay* sistemos naujame įrenginyje buvo pridėta, suvedus pareiškėjos mokėjimo kortelės personalizuotus saugumo duomenis, taip pat būtent į pareiškėjos mobilųjį telefoną siųstą vienkartinį saugos kodą. Nors pareiškėja teigia, kad šių duomenų tretiesiems asmenims neatskleidė, tačiau tiek iš banko pateiktų duomenų, tiek iš susiklosčiusios praktikos matyti, kad objektyviai nebuvo galima mokėjimo kortele atsiskaityti *Apple Pay* metodu, jeigu tretieji asmenys nebūtų žinoję mokėjimo kortelės duomenų ir *tik* į pareiškėjos mobilųjį telefoną siųsto vienkartinio saugos kodo.

Dėl šios priežasties, pareiškėja, galimai nesuprasdama atliekamų veiksmų reikšmės bei pasekmių, tikėtina turėjo atskleisti tretiesiems asmenims visus duomenis, būtinus jos mokėjimo kortelei pridėti prie *Apple Pay* sistemos naujame įrenginyje, iš kurio vėliau ir inicijuota pareiškėjos neautorizuota Operacija. Pareiškėjai perdavus tretiesiems asmenims SMS žinute jos telefono numeriu atsiųstą saugos kodą, mokėjimo kortelės pridėjimas naujame įrenginyje buvo patvirtintas, o atsiskaitymo *Apple Pay* paslauga aktyvuota – ja naudojantis ir inicijuota bei patvirtinta ir Operacija gavėjui *Selfridges*, kurios suma pareiškėjai nėra iki šiol grąžinta.

Kaip nurodoma atsiliepime, be pareiškėjos telefono numeriu išsiųsto vienkartinio saugos kodo suvedimo į *Apple Pay* sistemą, pareiškėjos mokėjimo kortelės pridėjimas nebūtų buvęs

[3] https://www.revolut.com/lt-LT/legal/terms/

[4] Lietuvos Aukščiausiojo Teismo Civilinių bylų skyriaus teisėjų kolegijos 2008 m. rugpjūčio 25 d. nutartis civilinėje byloje Nr. 3K-3-304/2008; 2009 m. kovo 16 d. nutartis civilinėje byloje Nr. 3K-3-101/2009 ir kt.

patvirtintas ir atsiskaitymas su *Apple Pay* būtų buvęs neįmanomas: įvedus neteisingą saugos kodą, visas procesas yra pradedamas iš naujo, tai yra, vėl prašoma suvesti mokėjimo kortelės duomenis, ši informacija perduodama mokėjimo paslaugų teikėjui, ją patvirtinus yra išsiunčiamas naujas vienkartinis saugos kodas SMS žinute.

Taip pat svarbu pažymėti ir tai, kad ginčo nagrinėjimo metu bankas pateikė duomenis, kad siunčiant vienkartinį saugos kodą, pareiškėjai SMS žinutėje papildomai buvo nurodyta šio kodo paskirtis bei perspėjimas šio kodo neperduoti tretiesiems asmenims[5]. Šios aplinkybės patvirtina, kad bankas, siekdamas užtikrinti, kad pareiškėja tinkamai įvertintų vienkartinio saugos kodo paskirtį ir neperduotų jo tretiesiems asmenis, informavo apie tai pareiškėją, tačiau pareiškėja nekreipė dėmesio į SMS žinutės turinį ir tikėtina perdavė tretiesiems asmenims tik jai vienai siųstą ir žinomą vienkartinį saugos kodą.

Atkreiptinas dėmesys ir į tai, kad ginčo nagrinėjimo metu nebuvo nustatyta duomenų, kurių pagrindu būtų galima įžvelgti įsilaužimo į pareiškėjos sąskaitą, pareiškėjos duomenų atskleidimo, banko sistemų trikdžių ar neveikimo požymių. Dėl šios priežasties, darytina išvada, kad nagrinėjamu atveju mokėjimo kortelės duomenis ir vienkartinį saugos kodą labiausiai tikėtina, kad tretiesiems asmenims turėjo atskleisti pati pareiškėja.

Išanalizavus šias bei visas kitas ginčo nagrinėjimo metu 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 ginčo nagrinėjimo metu nustatytų aplinkybių, Operaciją 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 bei tretiesiems asmenims suteikė vienkartinį saugos kodą, kurį gavo į sau priklausantį telefono numerį trumpąją SMS žinute.

Todėl, 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 Operaciją

Pareiškėja kreipimesi teigia, kad supratusi, jog tapo sukčių auka, iškart ėmėsi priemonių tam, kad atšauktų Operaciją, t. y. naudodamasi *Revolut* mobiliąja programėle, susisiekė su banku ir informavo apie ginčijamą Operaciją bei užpildė banko nurodytą prašymą dėl lėšų grąžinimo procedūros inicijavimo.

Vertinant pareiškėjos teiginius dėl Operacijos atšaukimo ir jos sumos į pareiškėjos sąskaitą banke grąžinimo, 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

[5] SMS žinutės tekstas anglų kalba: „Revolut verification code for *Apple Pay*: *******. Never share it with anyone, ever.“

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".

Remiantis tiek pareiškėjos, tiek banko pateiktais paaiškinimais, matyti, kad pareiškėja dėl atlikos ginčijamos Operacijos kreipėsi jau po to, kai Operacija buvo tinkamai autorizuota tarp šalių sudarytoje sutartyje sutarta forma ir tvarka ir negalėjo būti atšaukta po to, kai ją gavo pareiškėjos mokėjimo paslaugų teikėjas, šiuo atveju – bankas, todėl bankas, remiantis pirmiau minėtomis Mokėjimų įstatymo ir Sąlygų nuostatomis, neturėjo pareigos įvykdyti pareiškėjos prašymo atšaukti Operaciją, praėjus įstatyme nustatytam jo atšaukimo terminui ir (ar) grąžinti į pareiškėjos sąskaitą šios mokėjimo sumos.

Taigi, įvertinus visa tai, kas išdėstyta pirmiau, ir nustačius, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, darytina išvada, kad pareiškėjos banko atžvilgiu keliamas reikalavimas grąžinti ir (ar) kompensuoti Operacijos sumą – 9330 GBP, 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.

Direktorius Arūnas Raišutis