LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

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

2023-03-29 Nr. 429-170
Vilnius

Lietuvos bankas gavo X. X. (toliau – pareiškėjas) kreipimąsi, kuriuo prašoma išnagrinėti tarp pareiškėjo ir *Revolut Bank UAB* (toliau – bankas) kilusį ginčą.

N u s t a t y t a:

2023 m. sausio 6 d. 19 val. 47 min. banko pareiškėjui išduota *VISA* mokėjimo kortele Nr. (*duomenys neskelbiami*), panaudojant *Apple Pay* mokėjimo metodą, įvykdytos dvi mokėjimo operacijos, kurių suma 4 900 Eur, gavėjui *Coinbase Ireland* (toliau – Operacijos).

Tą pačią dieną pareiškėjas kreipėsi į banką ir nurodė, kad galimai tapo sukčių auka. Pareiškėjas teigė, kad į savo mobilųjį telefoną gavo trumpąją SMS žinutę, kurioje buvo nurodyta, kad jo mokėjimo sąskaitoje yra bandoma inicijuoti mokėjimo operaciją ir pateikiama aktyvi nuoroda į tinklalapį „rev-ireland.com“. Pareiškėjas nurodė, kad paspaudė aktyvią nurodą, todėl buvo nukreiptas į tariamą banko tinklalapį, jame suvedė banko PIN kodą. Be to, pareiškėjas teigė, kad su juo papildomai susisiekė tretieji asmenys ir nurodė, kad pareiškėjo sąskaitoje yra vykdoma neteisėta veikla. Pareiškėjas taip pat bankui atskleidė, kad galėjo tretiesiems asmenims atskleisti jam trumpąja SMS žinute atsiųstą banko kodą, kuris buvo skirtas jo mokėjimo kortelės pridėjimui prie *Apple Pay* patvirtinti.

Gavęs pareiškėjo kreipimąsi, bankas pradėjo vidinį tyrimą dėl galimo sukčiavimo. Įvertinęs pareiškėjo pateiktus duomenis, bankas pakartotinai kreipėsi į pareiškėją ir prašė pateikti jam atsiųstų trumpųjų SMS žinučių ekrano nuotraukas, kuriose matytųsi gautų pranešimų turinys. Bankas pasiūlė pareiškėjui užpildyti prašymą dėl lėšų grąžinimo procedūros (angl. *chargeback*) inicijavimo.

Pareiškėjas bankui pateikė duomenis, iš kurių matyti, kad pareiškėjas buvo nukreiptas į puslapį, kuriame turėjo suvesti savo personalizuotus saugumo duomenis, t. y. įvesti banko programėlės PIN kodą.

2023 m. sausio 7 d. pareiškėjas taip pat pateikė lėšų grąžinimo prašymą, tačiau bankas, įvertinęs visus surinktus duomenis, jį atmetė. Bankas tokį sprendimą priėmė, nes nustatė, kad nebuvo rasta jokių apgaulingos veiklos pareiškėjo atsiskaitomoje sąskaitoje požymių, todėl už Operacijų atlikimą atsakingas turėtų būti būtent pats pareiškėjas.

Sužinojęs banko sprendimą, pareiškėjas 2023 m. sausio 7 d. kreipėsi į banką ir prašė sprendimą apsvarstyti pakartotinai, tačiau bankas 2023 m. sausio 12 d. pareiškėjui pateikė atsakymą, kuriame nurodė, kad priimtas sprendimas yra pagrįstas ir keičiamas nebus. Pareiškėjas su tuo nesutiko, todėl tarp šalių kilo ginčas.

Kreipimesi į Lietuvos banką pareiškėjas prašo grąžinti Operacijų metu iš pareiškėjo atsiskaitomosios sąskaitos nurašytas lėšas, t. y. grąžinti 4 900 Eur. Pareiškėjas kreipimesi į Lietuvos banką pateikė tokius pat duomenis, kokius pateikė kreipdamasis į banką. Pareiškėjo teigimu, jam tretieji asmenys skambino 2023 m. sausio 6 d. 19 val. 54 min., taigi, po to, kai Operacijos jau buvo įvykdytos. Vienkartinį saugos kodą pareiškėjas perdavė tik po to, kai Operacijos buvo atliktos, todėl Operacijos negalėjo būti įvykdytos būtent tuo metu, t. y. 2023 m. sausio 6 d. 19 val. 47 min. Be to, Operacijos buvo atliktos naudojant *Apple Pay* mokėjimo metodą, tačiau pareiškėjas naudoja *Samsung* telefoną. Pareiškėjas teigia iš karto po to, kai Operacijos buvo atliktos, kreipęsis į banką, todėl bankas turėjo galimybę atšaukti Operacijas ir nepervesti lėšų tretiesiems asmenims.

Atsiliepime į pareiškėjo kreipimąsi bankas nurodo nesutinkąs su pareiškėjo reikalavimu ir

prašo jį atmesti. Banko teigimu, Operacijos buvo atliktos mobiliuoju įrenginiu, kurio pavadinimas – „aVBob25l“. 2023 m. sausio 6 d. šis mobilusis įrenginys, kaip *Apple pay* mokėjimo įrenginys, buvo pridėtas prie *Apple Pay* ir autorizuotas paties pareiškėjo. Bankas nurodo, kad, norėdamas 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 kortelės pridėjimą, įvedant vienkartinį saugos kodą, gautą trumpąja SMS žinute. Banko teigimu, žinutė su vienkartiniu kodu visais atvejais yra siunčiama į telefono numerį, kuris buvo nurodytas ir autorizuotas vartotojo sudarant sutartį su banku. Šiuo atveju apsaugos žinutė buvo išsiųsta pareiškėjo nurodytu numeriu, kurį pareiškėjas patvirtino registruojant paskyrą ir sudarant sutartį su banku. Bankas akcentavo, kad toks saugumo kriterijus neleidžia tretiesiems asmenims pasinaudoti mokėjimo kortele, be vartotojo žinios pridėti mokėjimo kortelę prie įrenginio ir atlikti mokėjimo operacijas.

Banko teigimu, kartu su vienkartiniu saugos kodu pareiškėjui trumpojoje SMS žinutėje buvo nurodyta šio kodo paskirtis bei perspėjimas šio kodo neperduoti tretiesiems asmenims, tačiau pareiškėjas elgėsi nepakankamai apdairiai, nes atskleidė vienkartinį kodą tretiesiems asmenims. Bankas atkreipia dėmesį į tai, kad, nesuvedus vienkartinio saugos kodo į *Apple Pay*, pareiškėjo mokėjimo kortelės pridėjimas nebūtų buvęs patvirtintas ir atsiskaitymai su *Apple Pay* būtų buvę neįmanomi. Bankas nurodo neteigiantis, kad pareiškėjas pats naudojosi *Apple Pay*, tačiau iš turimų sistemų duomenų akivaizdu, kad pareiškėjo mokėjimo priemonė prie *Apple Pay* galėjo būti ir buvo pridėta pareiškėjui atskleidus tik jam žinomą informaciją (mokėjimo kortelės duomenis ir vienkartinį saugos kodą). Banko teigimu, pareiškėjas pats tretiesiems asmenims atskleidė duomenis ir tokiais savo veiksmais patvirtino mokėjimo kortelės pridėjimą prie *Apple Pay*, taigi, elgėsi aplaidžiai ir nerūpestingai.

Bankas taip pat akcentuoja, kad iš tyrimo metu surinktos informacijos matyti, kad pareiškėjas ne tik leido mokėjimo kortelę pridėti prie *Apple P*ay, tačiau savo aktyviais veiksmais leido prisijungti ir prie pareiškėjo internetinės banko programėlės versijos ir pridėti internetinę naršyklę *Mozilla Firefox*, kaip antrinį įrenginį, prie pareiškėjo asmeninės sąskaitos. Bankas nurodo, kad tokie veiksmai galėjo būti atlikti tada, kai pareiškėjas paspaudė jam SMS žinute atsiųstą nuorodą ir suvedė atitinkamus duomenis, kurie susiję su prisijungimu prie interneto banko mobiliosios programėlės (PIN kodą). Banko teigimu, nors šie pareiškėjo veiksmai neturėjo įtakos Operacijoms, tačiau trečiojo asmens galimybė prisijungti prie pareiškėjo asmeninės mokėjimo sąskaitos be pareiškėjo aktyvių veiksmų nebūtų buvusi įmanoma, nes bankas į pareiškėjo mobilųjį telefoną išsiuntė įspėjimus ir prašymą patvirtinti, kad būtent jis jungiasi prie asmeninės sąskaitos per banko programėlės naršyklės versiją, todėl pareiškėjas turėjo galimybę suvokti, kokius veiksmus atlieka ir kad prie jo sąskaitos bando prisijungti sukčiai.

Atsižvelgdamas i visa tai, bankas mano, kad jam nekyla pareiga grąžinti tinkamai įvykdytų Operacijų lėšų, todėl prašo atmesti pareiškėjo reikalavimą kaip nepagrįstą.

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

Vadovaujantis Lietuvos banko valdybos 2012 m. sausio 26 d. nutarimu Nr. 03-23 patvirtintų Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių 45 punktu, vartojimo ginčai Lietuvos banke nagrinėjami laikantis rungimosi, ginčų nagrinėjimo operatyvumo, koncentracijos, ekonomiškumo ir bendradarbiavimo principų. Vartotojas ir finansų rinkos dalyvis privalo įrodyti tas aplinkybes, kuriomis remiasi kaip savo reikalavimų arba atsikirtimų pagrindu, išskyrus atvejus, kai remiamasi aplinkybėmis, kurių nereikia įrodinėti. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Pareiškėjo ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjui jo mokėjimo kortele, panaudojant *Apple Pay* mokėjimo metodą, atliktų Operacijų, kurių vertė 4 900 Eur ir kurių atlikti pareiškėjas teigia nedavęs sutikimo, sumą.

Pareiškėjas neigia autorizavęs Operacijas ir (ar) pridėjęs savo mokėjimo kortelę prie *Apple Pay* sistemos naujame įrenginyje ir tvirtina, kad lėšos iš jo atsiskaitomosios sąskaitos buvo nurašytos dėl to, kad tretieji asmenys galėjo pasisavinti pareiškėjo mokėjimo kortelės duomenis. Dėl šios priežasties pareiškėjas prašo banko grąžinti 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 pareiškėjo veiksmų, kuriais tretiesiems asmenims

buvo atskleisti pareiškėjo mokėjimo priemonių personalizuoti saugumo duomenys, dėl to tretieji asmenys įgijo galimybę savo įrenginiu inicijuoti Operacijas pareiškėjo 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 pareiškėjo ginčijamos Operacijos buvo atliktos naudojantis trečiųjų asmenų įrenginyje įdiegtu *Apple Pay* mokėjimo būdu, prie atitinkamo įrenginio, kuriame veikia *Apple Pay* sistema, pridėjus pareiškėjo mokėjimo kortelę. Taigi, šalių neginčijamomis aplinkybėmis, Operacijos buvo inicijuotos ir įvykdytos trečiųjų asmenų, jiems neteisėtu būdu sužinojus (pasisavinus) pareiškėjo mokėjimo priemonių personalizuotus saugumo duomenis ir juos panaudojus naujame įrenginyje pridedant pareiškėjo mokėjimo kortelę prie *Apple Pay* sistemos, o vėliau inicijuojant ir įvykdant Operacijas. Akivaizdu, kad Operacijų inicijavimas ir patvirtinimas neatitiko pačio pareiškėjo valios, nors formaliai (pagal išorinius požymius) ir sutapo su pareiškėjo ir banko sutarta sutikimo atlikti mokėjimo operacijas davimo forma ir tvarka.

Pareiškėjo nurodytos aplinkybės, kad Operacijos nėra pareiškėjo autorizuotos, o pareiškėjo mokėjimo kortelę prie *Apple Pay* sistemos naujame įrenginyje pridėjo ne pareiškėjas, o tretieji asmenys, bankas atsiliepime neginčija, todėl nagrinėdamas šį ginčą Lietuvos bankas daro išvadą, kad Operacijos, atliktos nesant pareiškėjo valios, jam net nežinant apie inicijuojamas Operacijas ir neišreiškus jokių valinių veiksmų patvirtinti Operacijas , laikytinos neautorizuotomis.

Siekiant išspręsti tarp pareiškėjo ir banko kilusį ginčą bei pasisakyti dėl pareiškėjo keliamų reikalavimų pagrįstumo, Lietuvos banko vertinimu, būtina nustatyti ar: 1) dėl neautorizuotų Operacijų bankas privalo pareiškėjui kompensuoti jo patirtus nuostolius; 2) bankas turėjo galimybę ir pareigą atšaukti Operacijas.

1. Dėl neautorizuotų Operacijų pasekmių ir pareiškėjo teisės į Operacijų 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 pareiškėjas galėjo veikti nesąžiningai arba tyčia, įskaitant sukčiavimą, nėra. Tai reiškia, kad, siekiant įvertinti, ar bankas pagrįstai atsisako kompensuoti pareiškėjo nuostolius, susijusius su Operacijų įvykdymu, ir ar galėtų pareiškėjo atžvilgiu būti taikoma Mokėjimų įstatymo 39 straipsnio 3 dalis, būtina nustatyti, ar pareiškėjo 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 pareiškėjo neatsargumas, dėl kurio visi jo reikalaujami atlyginti nuostoliai turėtų tekti pačiam pareiškėjui.

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.“[1]

Bankas mano, kad nuostolius dėl Operacijų pareiškėjas patyrė dėl savo didelio neatsargumo, nes, perduodamas tretiesiems asmenims savo mokėjimo kortelės duomenis (mokėjimo kortelėje nurodytus savo vardą, pavardę, kortelės numerį ir CVV kodą) bei vienkartinį banko pareiškėjui jo 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 taip suteikė galimybę tretiesiems asmenims mokėjimo kortelės sąskaitoje vykdyti Operacijas pareiškėjo 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, arba būdamas labai neatsargus.

Taigi, banko sprendimas nekompensuoti pareiškėjo nuostolių dėl neautorizuotų Operacijų įvykdymo galėtų būti vertinamas kaip pagrįstas tik tuo atveju, jei būtų įrodyta, kad pareiškėjas, atskleisdamas tam tikrus personalizuotus savo mokėjimo priemonių saugumo duomenis ir taip įgalindamas trečiuosius asmenis panaudoti šiuos duomenis pareiškėjo mokėjimo kortelei prie *Apple Pay* sistemos naujame mobiliajame įrenginyje pridėti, o vėliau ir inicijuoti Operacijas, elgėsi itin aplaidžiai – buvo labai neatsargus.

Kaip jau buvo minėta pirmiau, Mokėjimų įstatymo 34 straipsnyje reglamentuota viena iš mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigų – naudotis

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

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[2]".

Taigi, pirmiau aptartos Sąlygų nuostatos aiškiai nustato, kad už mokėjimo ir tapatybės patvirtinimo priemonių personalizuotų saugumo duomenų konfidencialumą yra atsakingas mokėtojas, šiuo atveju – pareiškėjas, jis privalo užtikrinti, kad minėti duomenys netaptų žinomi tretiesiems asmenims. Atsižvelgiant į tai, manytina, kad pareiškėjo elgesys būtų laikomas kaip atitinkantis mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, jei būtų nustatyta, kad pareiškėjas ėmėsi adekvačių veiksmų (ar 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.

Lietuvos bankas, įvertinęs abiejų šalių pateiktus duomenis, nustatė, kad pareiškėjas dar iki atliekant Operacijas kontaktavo su trečiaisiais asmenimis, nes 2023 m. sausio 6 d. 19 val. 07 min. gavo įtartino pobūdžio SMS žinutę dėl neautorizuoto mokėjimo ir paspaudė žinutėje pateiktą nuorodą. Iš pateiktų duomenų matyti, kad pareiškėjas 2023 m. sausio 6 d. 19 val. 17 min. gavo vienkartinį saugos kodą, kurį turėjo pateikti tretiesiems asmenims, nes tą pačią minutę mokėjimo kortelė buvo sėkmingai pridėta prie *Apple Pay* paslaugą palaikančio įrenginio, o po 30 min. buvo atliktos Operacijos, kurių metu buvo pasisavintos pareiškėjo lėšos.

Bankas kartu su atsiliepimu Lietuvos bankui pateikė vidinės sistemos duomenis, kurie patvirtina, kad pareiškėjo ginčijamos Operacijos mokėjimo kortele buvo inicijuotos 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, tai, banko pateiktais įrodymais, ir buvo atlikta šiuo atveju. Pareiškėjas nurodo, kad trečiųjų asmenų skambutis buvo vėliau, kai Operacijos jau buvo atliktos, todėl pareiškėjas tik tuo metu galėjo vienkartinį saugos kodą atskleisti sukčiams.

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[3].

Kaip jau minėta, ginčo byloje esančiais duomenimis, pareiškėjo mokėjimo kortelė prie *Apple Pay* sistemos naujame įrenginyje buvo pridėta, suvedus pareiškėjo mokėjimo kortelės personalizuotus saugumo duomenis, taip pat būtent į pareiškėjo mobilųjį telefoną siųstą vienkartinį saugos kodą. Nors pareiškėjas teigia, kad šių duomenų tretiesiems asmenims neatskleidė arba atskleidė jau po Operacijų įvykdymo, tačiau iš banko pateiktų duomenų, matyti, kad objektyviai nebuvo galima pridėti mokėjimo kortelės prie *Apple Pay* ir atsiskaityti šiuo metodu, jeigu tretieji asmenys nebūtų žinoję mokėjimo kortelės duomenų ir tik į pareiškėjo mobilųjį telefoną siųsto vienkartinio saugos kodo. Įvedus neteisingą vienkartinį 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.

Be to, bankas pateikė duomenis, kad, siunčiant vienkartinį saugos kodą, pareiškėjui SMS žinutėje papildomai buvo nurodyta šio kodo paskirtis bei perspėjimas šio kodo neperduoti tretiesiems asmenims, net jeigu šie asmenys ir tvirtina esantys banko darbuotojai[4]. Šios

---

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

[3] 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.

[4] SMS žinutės tekstas anglų kalba: „This code will be used to add your card to another Apple 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

aplinkybės patvirtina, kad bankas, siekdamas, kad pareiškėjas tinkamai įvertintų vienkartinio saugos kodo paskirtį ir neperduotų jo tretiesiems asmenis, informavo apie tai pareiškėją, tačiau pats pareiškėjas teigia nekreipęs dėmesio į SMS žinutės turinį ir perdavęs tretiesiems asmenims tik jam vienam siųstą ir žinomą vienkartinį saugos kodą.

Atkreiptinas dėmesys ir į tai, kad nagrinėjant ginčą nebuvo nustatyta duomenų, kurių pagrindu būtų galima įžvelgti pareiškėjo duomenų atskleidimo, banko sistemų trikdžių ar neveikimo požymių. Dėl šios priežasties darytina išvada, kad labiau tikėtina, kad pareiškėjas, galimai nesuprasdamas atliekamų veiksmų reikšmės bei pasekmių, dar iki atliekant Operacijas atskleidė tretiesiems asmenims visus duomenis, būtinus jo mokėjimo kortelei pridėti prie *Apple Pay* sistemos naujame įrenginyje, iš kurio vėliau ir inicijuotos pareiškėjo neautorizuotos Operacijos. Pareiškėjui perdavus tretiesiems asmenims SMS žinute jo telefono numeriu atsiųstą saugos kodą, mokėjimo kortelės pridėjimas naujame įrenginyje buvo patvirtintas, o atsiskaitymo *Apple Pay* paslauga aktyvuota – ja naudojantis ir inicijuotos bei patvirtintos Operacijos.

Be to, dar iki atliekant Operacijas pareiškėjas aktyviais veiksmais suteikė galimybę tretiesiems asmenims prisijungti prie internetinės banko programėlės versijos.

Iš banko pateiktų duomenų matyti, kad tretieji asmenys prie internetinės banko programėlės versijos prisijungė įvesdami pareiškėjo telefono numerį, kuris buvo nurodytas bankui atidarant mokėjimo sąskaitą, o vėliau buvo patvirtintas pareiškėjo mobiliajame telefone įvedus tik pareiškėjui žinomą PIN kodą[5].

Pareiškėjui įvedus PIN kodą, jo mobiliajame įrenginyje pasirodė iššokantis pranešimas, informuojantis apie bandymą prisijungti prie pareiškėjo paskyros ir prašantis patvirtinti, kad tai norėjo atlikti pareiškėjas[6]. Pareiškėjui paspaudus iššokantį pranešimą, pareiškėjo mobiliajame įrenginyje atsidarė autorizacijos langas, kuriame buvo atitinkamo pobūdžio informacija, leidžianti identifikuoti siekiančio prisijungti asmens vietą, naršyklę ir IP adresą. Taip pat pareiškėjui buvo matomas tekstas, kad yra mėginama prisijungti prie pareiškėjo asmeninės mokėjimo sąskaitos per internetinę banko programėlės versiją. Galiausiai nurodoma, kad jeigu tai atlieka ne pareiškėjas, toks prašymas turėtų būti atšauktas ir apie tai pareiškėjas turėtų informuoti banką[7]. Iš banko pateiktų duomenų matyti, kad pareiškėjas pasirinko patvirtinti prisijungimą, todėl įrenginys, iš kurio buvo bandoma prisijungti, buvo įtrauktas į įrenginių sąrašą kaip antrinis įrenginys.

Be to, pareiškėjui net ir į jo el. paštą buvo išsiųstas pranešimas, kad buvo aptiktas nežinomas įrenginys, su kuriuo yra bandoma prisijungti prie banko internetinės programėlės versijos. Pareiškėjui el. laiške buvo papildomai nurodyta atitinkamo pobūdžio informacija, leidžianti identifikuoti siekiančio prisijungti asmens vietą, naršyklę ir IP adresą. Taip pat nurodoma, kad jei ne pareiškėjas atlieka šiuos veiksmus, pareiškėjas turėtų nedelsdamas pakeisti savo prisijungimo slaptažodį ir kreiptis į banką[8].

Galiausiai, pareiškėjui patvirtinus trečiųjų asmenų prisijungimą prie jo asmeninės sąskaitos, jo mobiliajame įrenginyje pasirodė ir trečias pranešimas, kuris informavo, kad prie pareiškėjo sąskaitos buvo prisijungta iš naujo įrenginio, todėl, jeigu tai padarė ne pareiškėjas, jis turėtų pakeisti prisijungimo slaptažodį ir susisiekti su banku[9].

Lietuvos banko vertinimu, visuose trijuose pareiškėjui siųstuose pranešimuose ir el. laiške buvo aiškiai prašoma patvirtinti, kad būtent pareiškėjas, o ne tretieji asmenys siekia prisijungti prie pareiškėjo asmeninės sąskaitos per internetinę banko programėlės naršyklės versiją. Tačiau pareiškėjas nebuvo pakankamai atidus ir rūpestingas, ignoravo jam siunčiamus pranešimus, suvedė tik jam žinomą 4 skaitmenų PIN kodą ir taip savo aktyviais veiksmai leido tretiesiems asmenims prisijungti prie jo asmeninės sąskaitos per internetinę banko programėlės naršyklės versiją.

Lietuvos banko vertinimu, nors pareiškėjo atlikti veiksmai, kurie leido tretiesiems

---

a new device. Revolut verification code for Apple Pay: *******."

[5] Iš banko pateiktų duomenų matyti, kad 4 skaitmenų PIN kodas buvo suvestas iš pareiškėjo mobiliojo įrenginio SM-A4-05FN, kuris naudoja *Android* sistemą ir kuriuo pareiškėjas naudojosi prieš ir po Operacijų.

[6] Pareiškėjui rodomos žinutės tekstas: „*There was an attempted web access request. Tap to confirm this was you*".

[7] Pareiškėjui rodomas žinutės tekstas: „*Someone`s trying to log in to your account on the Revolut website. If it`s you, approve it. If it`s not you, reject it, and let us know, as your account may be at risk*".

[8] Pareiškėjui išsiųstas el. laiško tekstas: Unknown devi ce login. Hey [firstName], we`ve noticed that someone logged into your Revolut account from another device. Daitails of the log in are below. If this was you, no worries, go ahead and hit delete. If it was nor you, then your account may have been compromised, in this case please change your passcode immediately, then contact our in-app support to secure your account.

[9] Pareiškėjui rodomos tekstas: „*We`ve noticed a login attemt to your account from new device. If it wasn`t you, please change your passcode and contact support immediately*".

asmenims prisijungti prie pareiškėjo banko internetinės programėlės versijos tiesiogiai ir neturėjo įtakos Operacijoms, tačiau pareiškėjas jau šiuos veiksmus atlikdamas buvo informuotas apie galimą sukčiavimo riziką, tačiau nepaisė siųstuose pranešimuose pateiktų įspėjimų, tai nesukėlė jam įtarimų ir jis nesudvejojo dėl tolimesnių savo veiksmų, kurie lėmė, kad prie *Apple Pay* buvo pridėta mokėjimo kortelė.

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

Kaip matyti iš nustatytų aplinkybių, Operacijas tretieji asmenys be pareiškėjo žinios galėjo atlikti tik dėl to, kad pareiškėjas, būdamas labai neatsargus, netinkamai įvykdė Mokėjimų įstatyme (34 straipsnis) ir su banku sudarytoje sutartyje įtvirtintus mokėjimo kortelės saugaus naudojimo reikalavimus. Nurodytos aplinkybės leidžia teigti, kad pareiškėjas būtent dėl savo didelio neatsargumo neišsaugojo jo vardu išduotos mokėjimo kortelės duomenų konfidencialumo: nesiėmė tų saugumo priemonių, kurių privalėjo imtis, kad būtų tinkamai apsaugoti jo internetinės banko sąskaitos prisijungimo ir suteiktos mokėjimo priemonės duomenys, leido tretiesiems asmenims prisijungti prie internetinės banko programėlės versijos, ignoravo jam siunčiamus pranešimus, kurie įspėjo, kad šiuos veiksmus gali atlikti sukčiai, o svarbiausia – tretiesiems asmenims perdavė vienkartinį saugos kodą, kurį gavo į sau priklausantį telefono numerį trumpąją SMS žinute, tai ir lėmė pareiškėjo mokėjimo kortelės pridėjimą prie *Apple Pay* sistemos ir Operacijų atlikimą

Konstatavus, kad pareiškėjas, nesilaikydamas jam, kaip mokėtojui, 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) pareiškėjui neautorizuotų Operacijų lėšų.

2. Dėl galimybės atšaukti Operacijas

Pareiškėjas kreipimesi teigia, kad supratęs, jog tapo sukčių auka, iškart ėmėsi priemonių tam, kad atšauktų Operacijas ir susigrąžintų dar pareiškėjo sąskaitoje tik rezervuotas lėšas, t. y., naudodamasis banko mobiliąja programėle, susisiekė su banku, informavo apie ginčijamas Operacijas ir užpildė banko nurodytą prašymą dėl lėšų grąžinimo procedūros inicijavimo.

Vertinant pareiškėjo teiginius dėl Operacijų atšaukimo ir jų sumos į pareiškėjo 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 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 pareiškėjo, tiek banko pateiktais paaiškinimais, matyti, kad pareiškėjas 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 pareiškėjo mokėjimo paslaugų teikėjas, šiuo atveju – bankas, todėl bankas, remiantis pirmiau minėtomis Mokėjimų įstatymo ir Sąlygų nuostatomis, neturėjo pareigos įvykdyti pareiškėjo prašymo atšaukti Operacijas, praėjus įstatyme nustatytam jų atšaukimo terminui, ir (ar) grąžinti į pareiškėjo 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 pareiškėjo bankui keliamas reikalavimas grąžinti ir (ar) kompensuoti Operacijos sumą – 4 900 Eur, 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 pareiškėjo X. X. reikalavimus.

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