LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

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

2024-03-14 Nr. 429-47
Vilnius

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

N u s t a t y t a:

Laikotarpiu nuo 2023 m. gruodžio 13 d. iki 2023 m. gruodžio 14 d. banko pareiškėjai išduotomis *VISA* mokėjimo kortelėmis Nr. *Duomenys neskelbtini* ir *Duomenys neskelbtini* (toliau – Kortelės), panaudojant *Apple Pay* mokėjimo metodą, įvykdyta devyniolika mokėjimo operacijų, kurių suma 6 060,44 GBP, skirtingiems lėšų gavėjams (toliau – Operacijos).

2023 m. gruodžio 14 d. pareiškėja kreipėsi į banką dėl neautorizuotų Operacijų įvykdymo. Pareiškėja nurodė sulaukusi skambučio iš trečiųjų asmenų, kurie teigė esantys banko atstovai, jiems atskleidusi Kortelių duomenis ir pasidalijusi asmenuke (angl. *selfie*).

Įvertinęs pareiškėjos pateiktus paaiškinimus, bankas kreipėsi į pareiškėją, kad ji pateiktų išsamesnę informaciją apie įvykį, dėl kurio buvo įvykdytos Operacijos.

Pareiškėja papildomai nurodė, kad su ja susisiekė tariamas banko saugumo pareigūnas ir pranešė, kad į pareiškėjos sąskaitą buvo įsilaužta. Pareiškėjos teigimu, trečiasis asmuo pasirodė patikimas, nes siekė užtikrinti mokėjimo sąskaitos saugumą. Pareiškėja suteikė jam Kortelių duomenis. Pareiškėja taip pat bankui pateikė savo mobiliojo įrenginio ekrano nuotraukas, kuriose buvo matyti, kad į jos telefoną buvo siųsti vienkartiniai saugos kodai, skirti Kortelėms prie *Apple Pay* sistemos pridėti.

Atsižvelgdamas į gautus duomenis, bankas užblokavo pareiškėjos nurodytas Korteles ir pasiūlė pareiškėjai pateikti prašymus dėl lėšų grąžinimo procedūrų (angl. *chargeback*) inicijavimo.

2023 m. gruodžio 14 d. ir 2023 m. gruodžio 15 d. pareiškėja pateikė 3 lėšų grąžinimo prašymus dėl visų Operacijų.

Bankas, įvertinęs visus surinktus duomenis, priėmė sprendimą pareiškėjos prašymus atmesti ir Operacijų metu pervestų lėšų pareiškėjai negrąžinti. Bankas savo sprendimą grindė tuo, kad nebuvo nustatyta jokių neteisėtos veiklos pėdsakų, Operacijos buvo patvirtintos, todėl bankas jas įvykdė. Bankas apie tokį priimtą sprendimą informavo ir pareiškėją.

Nesutikdama su banko priimtu sprendimu, 2023 m. gruodžio 18 d. pareiškėja pateikė pretenziją, kuria prašė persvarstyti banko priimtą sprendimą ir grąžinti Operacijų metu pervestas lėšas. Tačiau 2023 m. gruodžio 22 d. bankas pateikė pareiškėjai atsakymą, kuriame nurodė, kad priimtas sprendimas yra pagrįstas, todėl keičiamas nebus. Pareiškėja su tuo nesutiko, todėl tarp šalių kilo ginčas.

Kreipimesi į Lietuvos banką pareiškėja prašo įpareigoti banką grąžinti Operacijų metu iš pareiškėjos sąskaitos nurašytas lėšas, t. y. grąžinti 6 060,44 GBP. Pareiškėja kreipimesi į Lietuvos banką pateikė tokius pat duomenis kaip ir kreipimesi į banką, t. y. kad pareiškėja tapo sukčių auka ir iš jos sąskaitos buvo nurašytos lėšos. Pareiškėja papildomai pažymėjo, kad ji neatliko Operacijų, jos yra neautorizuotos, todėl bankas privalėjo atlikti išsamų tyrimą ir pareiškėjai grąžinti Operacijų metu prarastas lėšas.

Atsiliepime į pareiškėjos kreipimąsi bankas nurodo nesutinkąs su pareiškėjos reikalavimu ir prašo jį atmesti. Banko teigimu, Kortelės buvo pridėtos prie skirtingų mobiliųjų įrenginių[1].

[1] Mokėjimo kortelė Nr. *Duomenys neskelbtini* buvo pridėta prie mobiliojo įrenginio „*Duomenys neskelbtini*“, o mokėjimo

2023 m. gruodžio 13 d. šie mobilieji įrenginiai, kaip *Apple Pay* mokėjimo įrenginiai, buvo pridėti prie *Apple Pay* sistemos ir autorizuoti. Bankas nurodo, kad, norėdami 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 žinutės buvo išsiųstos pareiškėjos nurodytu numeriu, kurį pareiškėja patvirtino registruodama paskyrą ir sudarydama sutartį su banku. Bankas akcentavo, kad toks saugumo kriterijus neleidžia tretiesiems asmenims pasinaudoti mokėjimo kortele, be vartotojo žinios pridėti mokėjimo kortelės prie įrenginio ir atlikti mokėjimo operacijų.

Banko teigimu, kartu su vienkartiniais saugos kodais pareiškėjai trumposiose SMS žinutėse buvo nurodyta šių kodų paskirtis bei perspėjimas 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 *Apple Pay*, pareiškėjos Kortelių pridėjimas nebūtų buvęs patvirtintas ir atsiskaitymai su *Apple Pay* būtų buvę neįmanomi. Be to, atliekant Operacijas banko sistemos identifikavo Operacijas kaip įtartinas ir jas sustabdė, o Korteles užblokavo. Banko teigimu, Operacijos buvo stabdomos dėl galimai neteisėtos veiklos ir geolokacijos nesutapimo[2]. Bankas nurodo, kad nors Kortelės ir buvo užblokuotos, tačiau pareiškėja, naudodamasi banko mobiliąja programėle, jas atblokavo, o apsaugos funkciją deaktyvavo.

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

Ginčo nagrinėjimo Lietuvos banke metu, siekdamas išsiaiškinti Operacijų įvykdymo ir prieš pareiškėją galimai nukreiptos sukčiavimo atakos aplinkybes, Lietuvos bankas kreipėsi į pareiškėją ir prašė pateikti papildomos informacijos. 2024 m. kovo 7 d. pareiškėja pateikė tokius pat duomenis kaip kreipimesi į banką ir kreipimesi į Lietuvos banką.

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 ginčo šalių pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Pareiškėjos ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjai jos Kortelėmis, panaudojant *Apple Pay* mokėjimo metodą, atliktų Operacijų, kurių vertė 6 060,44 GBP ir kurių atlikti pareiškėja teigia nedavusi sutikimo, sumą.

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

---

kortelė Nr. *Duomenys neskelbtini* buvo pridėta prie įrenginių „*Duomenys neskelbtini*“ ir „*Duomenys neskelbtini*“.

[2] Bankas nurodė, kad geolokacijos nesutapimas (angl. *geolocation mismatch*) – tai apsaugos priemonė, kuri banko vidaus sistemoms padeda nustatyti, ar įrenginio, kuriuo administruojama asmeninė mokėjimo sąskaita ir mokėjimo kortelė, kuria yra atliekama mokėjimo operacija, yra toje pačioje vietoje, ar ne. Esant nesutapimui tarp vietų, banko vidaus sistemos blokuoja mokėjimo operaciją.

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 teigia, kad pareiškėjos ginčijamos Operacijos buvo atliktos naudojantis trečiųjų asmenų įrenginiuose įdiegtu *Apple Pay* mokėjimo būdu, prie atitinkamų įrenginių, kuriuose veikia *Apple Pay* sistema, pridėjus pareiškėjos Korteles. 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, kad prie *Apple Pay* sistemos būtų pridėtos pareiškėjos Kortelės, kuriomis pasinaudojant vėliau inicijuotos ir įvykdytos Operacijos. 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 ir kad pareiškėjos Korteles prie *Apple Pay* sistemos naujuose įrenginiuose pridėjo ne pareiškėja, o tretieji asmenys, bankas atsiliepime neginčija, todėl nagrinėdamas šį ginčą Lietuvos bankas daro išvadą, kad Operacijos, atliktos nesant pareiškėjos valios ir jai net nežinant apie Operacijų inicijavimo aplinkybę bei neišreiškus jokių valinių veiksmų patvirtinti Operacijas, laikytinos neautorizuotomis.

Siekiant išspręsti tarp pareiškėjos ir banko kilusį ginčą bei pasisakyti dėl pareiškėjos keliamų reikalavimų pagrįstumo, Lietuvos banko vertinimu, būtina nustatyti, ar, atsisakydamas grąžinti pareiškėjai Operacijos metu pervestas lėšas, bankas pagrįstai rėmėsi Mokėjimų įstatymo 39 straipsnio 3 dalimi.

Mokėjimų įstatymo 39 straipsnio 3 dalyje nustatyta, kad mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai, jeigu jis juos patyrė veikdamas nesąžiningai arba tyčia ar dėl didelio neatsargumo neįvykdęs vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų.

Taip pat svarbu pažymėti, kad Lietuvos Aukščiausiasis Teismas yra konstatavęs, kad įstatyme nustatyta tokia mokėtojo paslaugų teikėjo atsakomybės už neautorizuotą mokėjimą sistema, pagal kurią mokėtojas turi teisę į neautorizuotos operacijos sumos sugrąžinimą, o mokėtojo paslaugos teikėjas turi pareigą ją sugrąžinti, išskyrus atvejus, jei nustatoma, kad: 1) mokėtojas veikia nesąžiningai; 2) mokėtojas tyčia ar dėl didelio neatsargumo pažeidžia vieną ar kelias Mokėjimų įstatymo 34 straipsnyje nustatytas mokėtojo pareigas, susijusias su mokėjimo priemonėmis ir personalizuotais saugumo duomenimis. Nurodyta mokėtojo paslaugų teikėjo atsakomybės už neautorizuotą mokėjimą sistema reiškia griežtąją mokėtojo paslaugų teikėjo atsakomybę už atliktas neautorizuotas mokėjimo operacijas, t. y. atsakomybę be kaltės. Kita vertus, mokėtojo paslaugų teikėjo atsakomybė be kaltės neeliminuoja paties mokėtojo pareigos elgtis rūpestingai ir atsakingai. Jeigu mokėtojas elgiasi nesąžiningai arba tyčia ar dėl didelio neatsargumo pažeidžia įstatyme jam nustatytas pareigas, paslaugos teikėjas yra atleidžiamas nuo atsakomybės. Ne bet kokių mokėtojo pareigų nevykdymas yra pagrindas atleisti mokėtojo paslaugos teikėją nuo atsakomybės, o būtent Mokėjimų įstatymo 34 straipsnyje nustatytų mokėtojo pareigų, kurios susijusios su mokėjimo priemonėmis ir personalizuotais saugumo duomenimis, be to, paprastas mokėtojo neatsargumas nėra laikomas mokėtojo paslaugos teikėjo atleidimo nuo atsakomybės sąlyga[3].

Duomenų, kad nagrinėjamu atveju pareiškėja galėjo veikti nesąžiningai arba tyčia, nėra, todėl galimas mokėtojo sukčiavimas, kaip pagrindas atleisti mokėtojo mokėjimo paslaugų teikėją nuo pareigos atlyginti mokėtojui nuostolius dėl neautorizuotos mokėjimo operacijos įvykdymo, šiame sprendime atskirai nebus plačiau analizuojamas.

Taigi, sprendžiant, ar banko atsisakymas grąžinti pareiškėjai Operacijų sumą laikytinas pagrįstu, būtina įvertinti, ar pareiškėjos elgesys, atskleidžiant tretiesiems asmenims personalizuotus saugumo duomenis ir taip įgalinant trečiuosius asmenis panaudoti šiuos duomenis pareiškėjos Kortelėms prie *Apple Pay* sistemos naujuose mobiliuose įrenginiuose pridėti, o vėliau ir Operacijoms inicijuoti, vertintinas kaip didelis neatsargumas, dėl kurio su mokėjimo operacijos įvykdymu atsiradę nuostoliai, kaip nustatyta Mokėjimų įstatymo

[3] Lietuvos Aukščiausiojo Teismo 2023 m. rugsėjo 12 d. nutartis civilinėje byloje Nr. e3K-3-182-1075/2023, 44 punktas.

39 straipsnio 3 dalyje, tektų pačiai pareiškėjai.

Lietuvos Aukščiausiasis Teismas yra išaiškinęs, kad didelis neatsargumas pasireiškia neprotingu arba išskirtiniu rūpestingumo nebuvimu, kai asmuo nėra tiek rūpestingas, kiek akivaizdžiai būtina esamomis aplinkybėmis[4]. Didelis mokėtojo neatsargumas gali būti konstatuojamas tik tuomet, jei mokėtojas elgėsi labai nerūpestingai. Kad mokėtojas elgėsi labai nerūpestingai, turi įrodyti mokėjimo paslaugų teikėjas, pateikdamas konkrečius tokį elgesį pagrindžiančius įrodymus. Ši įrodinėjimo našta negali būti perkelta mokėtojui[5].

Dėl mokėtojo neatsargumo laipsnio vertinimo, pagrindinių jo kriterijų ir glaudaus ryšio su ginčo byloje nustatytų individualių specifinių aplinkybių visuma Lietuvos bankas yra ne kartą plačiau pasisakęs savo ginčų nagrinėjimo praktikoje[6], todėl šiame sprendime bus pasisakoma tik šiai konkrečiai ginčo bylai aktualiais aspektais.

Neautorizuotos mokėjimo operacijos įvykdymo atveju didelis neatsargumas yra sietinas su vienos ar kelių Mokėjimų įstatymo 34 straipsnyje mokėtojui nustatytų pareigų, susijusių su mokėjimo priemone ir personalizuotais saugumo duomenimis, nevykdymu. Kaip yra konstatavęs Lietuvos Aukščiausiasis Teismas, neautorizuotos mokėjimo operacijos atveju mokėjimo paslaugų teikėjas turi įrodyti ne tik tai, kad mokėtojas pažeidė vieną ar kelias Mokėjimų įstatymo 34 straipsnyje nustatytas mokėtojo pareigas, susijusias su mokėjimo priemonėmis ir personalizuotais saugumo duomenimis, bet ir kad tai padarė dėl didelio neatsargumo[7].

Mokėjimų įstatymo 34 straipsnis nustato mokėtojo pareigą naudotis jam išduota mokėjimo priemone (nagrinėjamu atveju – mokėjimo kortele) pagal jos išdavimą ir naudojimą reglamentuojančias sąlygas, o sužinojus apie jos praradimą, vagystę arba neteisėtą pasisavinimą ar neautorizuotą jos naudojimą, nedelsiant apie tai pranešti mokėjimo paslaugų teikėjui arba jo nurodytam subjektui (Mokėjimų įstatymo 34 straipsnio 1 dalis), taip pat pareigą, gavus mokėjimo priemonę, imtis veiksmų, kad būtų apsaugoti personalizuoti saugumo duomenys (Mokėjimų įstatymo 34 straipsnio 2 dalis).

Bankas mano, kad nuostolius dėl Operacijų pareiškėja patyrė dėl savo didelio neatsargumo – t. y. pareiškėja, perduodama tretiesiems asmenims savo Kortelių duomenis (Kortelėse nurodytus savo vardą, pavardę, Kortelių numerį ir CVV kodus) bei vienkartinius banko pareiškėjai jos nurodytu telefono numeriu siųstus Kortelių pridėjimo prie *Apple Pay* sistemos saugos kodus, suteikė leidimą tretiesiems asmenims pridėti Korteles prie jų faktiškai valdomuose įrenginiuose įdiegto *Apple Pay* atsiskaitymo būdo ir taip suteikė galimybę tretiesiems asmenims Kortelių sąskaitoje vykdyti Operacijas pareiškėjos vardu.

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.[8]"

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 bei papildomai pateiktoje informacijoje ir banko atsiliepime nurodytas aplinkybes bei kartu su kreipimusi ir atsiliepimu pateiktus duomenis, nustatė, kad į pareiškėją prieš Operacijų įvykdymą telefonu kreipėsi tretieji asmenys, kurie prisistatė banko darbuotojais. Pareiškėja teigia, kad banko darbuotojai nurodė, kad jos mokėjimo sąskaitoje yra atliekami sukčiavimo veiksmai, todėl tam, kad būtų apsaugotos pareiškėjos lėšos, prašė perduoti pareiškėjos personalizuotus saugumo duomenis.

---

[4] Lietuvos Aukščiausiojo Teismo 2017 m. balandžio 13 d. nutartis civilinėje byloje Nr. e3K-3-180-378/2017.
[5] Lietuvos Aukščiausiojo Teismo 2023 m. rugsėjo 12 d. nutartis civilinėje byloje Nr. e3K-3-182-1075/2023, 82 punktas.
[6] Pavyzdžiui, ginčo bylos Nr. 2022-00586 ir 2022-02496.
[7] Lietuvos Aukščiausiojo Teismo 2023 m. rugsėjo 12 d. nutartis civilinėje byloje Nr. e3K-3-182-1075/2023, 78 punktas.
[8] https://www.revolut.com/lt-LT/legal/terms/

Iš pareiškėjos pateiktų paaiškinimų matyti, kad pareiškėja atliko visus trečiųjų asmenų nurodomus veiksmus.

Bankas kartu su atsiliepimu Lietuvos bankui pateikė vidinės sistemos duomenis, kurie patvirtina, kad pareiškėjos ginčijamos Operacijos Kortelėmis 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, pagal banko pateiktus įrodymus, ir buvo atlikta abiejų Kortelių atvejais. Aplinkybę, kad tretieji asmenys, tikindami, kad pareiškėjos mokėjimo sąskaitoje vyksta sukčiavimo veiksmai, prašė pateikti personalizuotus saugumo duomenis, pripažįsta ir pati pareiškėja.

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[9].

Vadinasi, ginčo byloje esančiais duomenimis, pareiškėjos Kortelės prie *Apple Pay* sistemos naujuose įrenginiuose buvo pridėtos, suvedus pareiškėjos Kortelių personalizuotus saugumo duomenis, taip pat būtent į pareiškėjos mobilųjį telefoną siųstus vienkartinius saugos kodus. Nors pareiškėja tiesiogiai savo kreipimesi nenurodo, kad tretiesiems asmenims perdavė į jos mobilųjį telefoną siųstus vienkartinius saugos kodus, tačiau tiek iš banko pateiktų duomenų, tiek iš susiklosčiusios praktikos matyti, kad objektyviai nebuvo galima pridėti Kortelių prie *Apple Pay* ir jomis atsiskaityti, jeigu tretieji asmenys nebūtų žinoję Kortelių duomenų ir *tik* į pareiškėjos mobilųjį telefoną siųstų vienkartinių saugos kodų. Be to, pati pareiškėja bankui pateikė savo mobiliojo įrenginio ekrano nuotraukas, kuriose matyti, kad būtent pareiškėjai buvo siunčiami vienkartiniai saugos kodai, kurie buvo reikalingi Kortelėms prie *Apple Pay* pridėti.

Dėl šios priežasties pareiškėja, galimai nesuprasdama atliekamų veiksmų reikšmės bei pasekmių, tikėtina, turėjo atskleisti tretiesiems asmenims visus duomenis, būtinus, kad jos Kortelės būtų pridėtos prie *Apple Pay* sistemos naujuose įrenginiuose, iš kurių vėliau ir inicijuotos pareiškėjos neautorizuotos Operacijos. Pareiškėjai perdavus tretiesiems asmenims SMS žinutėse jos telefono numeriu atsiųstus saugos kodus, Kortelių pridėjimas naujuose įrenginiuose buvo patvirtintas, o atsiskaitymo *Apple Pay* paslauga aktyvuota – ja naudojantis inicijuotos bei patvirtintos Operacijos, kurių suma pareiškėjai nėra iki šiol grąžinta.

Kaip nurodoma banko atsiliepime, be pareiškėjos telefono numeriu išsiųstų vienkartinių saugos kodų suvedimo į *Apple Pay* sistemą pareiškėjos Kortelių pridėjimas nebūtų buvęs patvirtintas ir atsiskaitymai naudojantis *Apple Pay* metodu būtų buvęs neįmanomi: 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.

Banko pateiktais duomenimis, siunčiant vienkartinius saugos kodus, pareiškėjai SMS žinutėse papildomai buvo nurodyta šių kodų paskirtis bei perspėjimas šių kodų neperduoti tretiesiems asmenims[10]. Šios aplinkybės patvirtina, kad bankas, siekdamas užtikrinti, kad pareiškėja tinkamai įvertintų vienkartinių saugos kodų paskirtį ir neperduotų jų tretiesiems asmenims, informavo apie tai pareiškėją, tačiau pareiškėja nekreipė dėmesio į SMS žinučių turinį ir perdavė tretiesiems asmenims tik jai vienai siųstus ir žinomus vienkartinius saugos kodus.

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.

Be to, iš banko pateiktų objektyvių duomenų matyti, jog prieš Operacijų atlikimą ir jų inicijavimo metu banko saugumo sistemos identifikavo Operacijas kaip įtartinas, jas sustabdė,

---

[9] 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.

[10] SMS žinutės tekstas anglų kalba: „This code will be used to add your card to another Apple pay device. Don't enter it anywhere unless you want to add your card to a new device. Don't share this code with anyone, even if they claim to be from Revolut. Revolut verification code for Apple pay: xxxxxx."

o Korteles užblokavo. Iš banko pateiktų paaiškinimų matyti, kad Operacijos buvo stabdomos dėl galimai neteisėtos veiklos ir dėl to, kad nesutapo mobiliojo įrenginio, kuriuo administruojama pareiškėjos asmeninė mokėjimo sąskaita, ir Kortelių, kuriomis yra atliekama mokėjimo operacija, vieta. Tačiau iš banko pateiktų duomenų matyti, kad nors bankas užblokavo Korteles, tačiau pareiškėja, naudodamasi banko mobiliąja programėle, jas atblokavo ir banko saugumo sistemos funkciją deaktyvavo. Taigi, Lietuvos banko vertinimu, minėti duomenys patvirtina, kad bankas, būdamas savo srities profesionalas, dėjo pastangas tam, kad apsaugotų pareiškėjos mokėjimo sąskaitoje esančias lėšas, tačiau pareiškėja pati savo iniciatyva atblokavo Korteles, deaktyvavo banko saugumo sistemas ir tokiais savo veiksmais leido tretiesiems asmenims inicijuoti ir patvirtinti Operacijas.

Išanalizavęs visas 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 galimybės.

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 išduotų Kortelių duomenų konfidencialumo – nesiėmė tų saugumo priemonių, kurių privalėjo imtis, kad būtų tinkamai apsaugoti jai suteiktų mokėjimo priemonių duomenys, ir tretiesiems asmenims suteikė vienkartinius saugos kodus, kuriuos gavo į sau priklausantį telefono numerį trumposiomis SMS žinutėmis, o prieš Operacijų atlikimą ir Operacijų atlikimo metu savo aktyviais veiksmais atblokavo Korteles ir deaktyvavo banko taikomas saugumo sistemas.

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 neautorizuotų Operacijų lėšų.

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 grąžinti ir (ar) kompensuoti Operacijų sumą – 6 060,44 GBP, yra nepagrįstas, todėl atmetamas.

Remdamasi tuo, kas išdėstyta, ir vadovaudamasi 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 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.

Finansinių paslaugų ginčų nagrinėjimo
skyriaus vadovė, pavaduojanti direktorių Rasa Cicėnienė