LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

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

2023 m. gegužės 10 d. Nr. 429-270
Vilnius

Lietuvos bankas gavo 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:

2022 m. gruodžio 27 d. pareiškėja, naudodamasi banko mobiliąja programėle, susisiekė su banko klientų aptarnavimo specialistais ir informavo, kad tapo sukčiavimo auka. Pareiškėja nurodė, kad jai paskambino asmuo, prisistatęs „Revolut" darbuotoju, ir ji jam suteikė informaciją apie vienkartinius saugumo kodus, skirtus „mokėjimo kortelės autorizacijai". Pareiškėja taip pat paminėjo, kad dieną prieš tai gavo SMS žinutę iš „Royal Mail" ir, paspaudusi gautą nuorodą, suvedė savo kortelės duomenis. Pareiškėja patikslino, kad jos mokėjimo kortele (*duomenys neskelbtini*) (toliau – Mokėjimo kortelė) buvo neteisėtai atliktos dvi mokėjimo operacijos, kurių bendra vertė – 2 590 GBP (toliau – Ginčijami mokėjimai).

Banko patarta, pareiškėja 2022 m. gruodžio 27 d. užpildė ir pateikė bankui prašymus dėl lėšų grąžinimo procedūros (angl. *chargeback*) inicijavimo Ginčijamų mokėjimų atžvilgiu.

2022 m. gruodžio 27 d. bankas priėmė sprendimą netenkinti pareiškėjos prašymų dėl lėšų grąžinimo procedūros inicijavimo, bankui įvertinus, kad pareiškėja yra atsakinga už Ginčijamų mokėjimų atlikimą, nes nežinomai trečiai šaliai suteikė vienkartinius saugos kodus, gautus SMS žinute. Pareiškėja apie šį sprendimą buvo informuota elektroniniu paštu tą pačią dieną.

Pareiškėja nesutinka su tokiu banko sprendimu, taip pat ir atsisakymu kitaip kompensuoti pareiškėjai dėl įvykdytų Ginčijamų mokėjimų atsiradusius nuostolius. Pareiškėja teigia buvusi apgauta trečiųjų asmenų ir neigia autorizavusi Ginčijamus mokėjimus ar siekusi jų įvykdymo. Pareiškėjai nesuprantama, kodėl buvo įmanoma pridėti jos Mokėjimo kortelę prie *Apple Pay* atsiskaitymo sistemos *iPhone* įrenginyje, nors pati pareiškėja naudojasi, taigi, ir banko mobiliąją programėlę turi, *Android* įrenginyje. Pareiškėja mano, kad bankas netinkamai įvykdė savo pareigą apsaugoti jos Mokėjimo kortelės sąskaitoje esančias lėšas, todėl kreipimesi prašo, kad bankas atlygintų pareiškėjos nuostolius dėl įvykdytų Ginčijamų mokėjimų.

Bankas nesutinka tenkinti pareiškėjos reikalavimo. Bankas mano, kad pareiškėjos Ginčijami mokėjimai buvo jos tinkamai autorizuoti, todėl bankas negali būti įpareigotas grąžinti pareiškėjai šių mokėjimų sumos. Bankas papildomai pažymi, kad pareiškėja, nepaisydama net kelis kartus gautuose SMS pranešimuose su vienkartiniais saugos kodais jos Mokėjimo kortelei prie *Apple Pay* mokėjimo sistemos pridėti nurodytos informacijos dėl šių kodų paskirties ir atidžiai neįvertinusi tariamo banko darbuotojo reikalavimo pateikti saugos kodą tapatybei patvirtinti, taigi, aplaidžiai ir nerūpestingai, pati savo aktyviais veiksmais trečiajam asmeniui suteikė galimybę pridėti jos mokėjimo priemonę prie *Apple Pay* įrenginio.

Atsižvelgdamas į išdėstytą informaciją ir argumentus, bankas prašė atmesti pareiškėjos reikalavimą.

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

Vadovaujantis Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių, patvirtintų Lietuvos banko valdybos 2012 m. sausio 26 d. nutarimu Nr. 03-23, 45 punktu, vartojimo ginčai Lietuvos banke nagrinėjami laikantis rungimosi, ginčų nagrinėjimo operatyvumo, koncentracijos, ekonomiškumo ir bendradarbiavimo principų. Vartotojas ir finansų rinkos dalyvis privalo įrodyti tas aplinkybes, kuriomis remiasi kaip savo

reikalavimų arba atsikirtimų pagrindu, išskyrus atvejus, kai remiamasi aplinkybėmis, kurių nereikia įrodinėti. Lietuvos bankas ginčo nagrinėjimo proceso metu neatlieka Lietuvos Respublikos Lietuvos banko įstatymo 42[1] straipsnyje reglamentuojamų patikrinimų, skirtų faktinėms aplinkybėms dėl Lietuvos banko priežiūrimo finansų rinkos dalyvio galimai padaryto Lietuvos banko kompetencijai priskirtų teisės aktų reikalavimų pažeidimo nustatyti ir įvertinti. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą ir jo pagrindu priima sprendimą.

Ginčas kilo dėl to, kad bankas atsisakė grąžinti pareiškėjai jos Mokėjimo kortele, naudojant *Apple Pay* mokėjimo nurodymo patvirtinimo metodą, atliktų Ginčijamų mokėjimų, kurių bendra vertė 2 590 GBP, sumą.

Pareiškėja teigia nedavusi sutikimo atlikti Ginčijamus mokėjimus, neigia juos autorizavusi ir (ar) pridėjusi savo mokėjimo kortelę prie *Apple Pay* sistemos iš naujo įrenginio. Pareiškėja teigia banko darbuotoju prisistačiusiam asmeniui atskleidusi tik SMS žinute gautą vienkartinį saugos kodą, ir to pakako, kad tretieji asmenys jos Mokėjimo kortelę pridėtų prie *Apple Pay* sistemos. Pareiškėjos manymu, bankas neužtikrino jos mokėjimo kortelės sąskaitoje esančių lėšų saugumo ir tai lėmė, kad Ginčijami mokėjimai buvo įvykdyti, o jų lėšos iš pareiškėjos mokėjimo kortelės sąskaitos buvo nurašytos. Bankas teigia, kad Ginčijami mokėjimai buvo įvykdyti naudojant *Apple Pay* mokėjimo nurodymo patvirtinimo metodą. Tam, kad pareiškėjos mokėjimo kortelė būtų pridėta prie *Apple Pay* sistemos, turėjo būti panaudoti pareiškėjos mokėjimo kortelės duomenys, o pridėjimas patvirtintas banko į sutartyje nurodytą telefono numerį išsiųstoje žinutėje pateiktu vienkartiniu saugos kodu. Banko vertinimu, Ginčijamus mokėjimus autorizavo pati pareiškėja arba pareiškėja dėl didelio neatsargumo atskleidė tretiesiems asmenims savo mokėjimo kortelės duomenis ir vienkartinį saugos kodą, dėl to tretieji asmenys galėjo įgyti galimybę inicijuoti Ginčijamus mokėjimus *Apple Pay* mokėjimo metodu.

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.

Siekiant išspręsti šį pareiškėjos ir banko ginčą, Lietuvos banko vertinimu, būtina nustatyti, ar: *1) Ginčijami mokėjimai laikytini autorizuotais; 2) bankas privalo grąžinti pareiškėjai Ginčijamų mokėjimų sumą; 3) pagrįstai pareiškėja teigia, kad banko paslaugos buvo teikiamos nesaugiai ir tai galėjo lemti pareiškėjos nuostolius*.

1. Dėl Ginčijamų mokėjimų autorizavimo

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).

Pažymėtina, kad Mokėjimų įstatyme nėra nustatytų konkrečių mokėtojo sutikimo įvykdyti mokėjimo operaciją būdų ir (arba) detalios tokio sutikimo davimo tvarkos. Vadovaujantis Mokėjimų įstatymo 13 straipsnio 3 dalies 3 punktu ir 29 straipsnio 1 punktu, mokėtojo sutikimo įvykdyti mokėjimo operaciją davimo sąlygos ir tvarka turi būti aptartos mokėtojo ir mokėjimo paslaugų teikėjo sudaromoje bendrojoje mokėjimo paslaugų teikimo sutartyje (toliau – bendroji sutartis).

Banko ir pareiškėjos bendrąją sutartį sudarančių banko privatiems klientams taikomų sąlygų 14 punkte nurodyta, kad mokėjimai gali būti autorizuojami įvedant mokėjimo kortelės duomenis (kortelės numerį, galiojimo datą, CVV kodą) arba PIN kodą. Sutikimas taip pat gali būti duotas paliečiant kortele terminalą (bekontaktis atsiskaitymas) ar atliekant kitus veiksmus su elektroniniu kortelių skaitytuvu. Šiuos veiksmus bankas laiko mokėtojo sutikimu atlikti mokėjimus iš banko sąskaitos[1]. Atsižvelgiant į tai, kad bendroji sutartis (ją sudarančios banko privatiems klientams taikomos sąlygos) nustato banko ir pareiškėjos tarpusavio santykius, ir

[1] Tekstas anglų k.: *„You can also make payments or withdraw cash using your Revolut Card. You can do this by entering the details of your Revolut Card (the card number, expiry date and CVC number) or your PIN. We will consider these actions as you giving consent to make payments or withdraw cash from your Revolut account. You also give your consent to make payments from your Revolut Card by: touching your Revolut Card at the terminal (a 'contactless' transaction) and taking other actions on the electronic card reader <…>"*

įvertinus tai, kad mokėjimo kortelės duomenys ir PIN kodo slaptažodis yra personalizuoti saugumo duomenys, kurie pripažįstami neskelbtinais mokėjimo duomenimis (Mokėjimų įstatymo 2 straipsnio 41 dalis), darytina išvada, kad bendrojoje sutartyje nurodyti mokėjimo operacijos autorizavimo būdai (suvedant mokėjimo kortelės duomenis ir (arba) PIN kodą) pareiškėjos ir banko santykiuose laikytini pareiškėjos sutikimu įvykdyti mokėjimo operaciją tik tada, kai pati pareiškėja pateikia mokėjimo kortelės duomenis ir (arba) suveda PIN kodo slaptažodį, norėdama įvykdyti mokėjimo operaciją.

Banko kartu su atsiliepimu pateiktais vidaus sistemos duomenimis, visi pareiškėjos Ginčijami mokėjimai atlikti tuo pačiu mobiliuoju įrenginiu (įrenginio pavadinimas matomas banko sistemose –„Tk's iPhone"), kuris kaip *Apple Pay* mokėjimo įrenginys prie *Apple Pay* sistemos buvo pridėtas ir autorizuotas, kaip nurodė bankas, pačios pareiškėjos prieš Ginčijamų mokėjimų inicijavimą būtent jų įvykdymo dieną, t. y. 2022 m. gruodžio 27 d.

Atsiliepime, net ir atsižvelgdamas į tai, kad Ginčijami mokėjimai buvo inicijuoti jų įvykdymo dieną, prie *Apple* Pay sistemos pridėjus pareiškėjos Mokėjimo kortelę naujame įrenginyje, kuris, kaip teigia bankas, nėra įprastai pareiškėjos naudojamas įrenginys, bankas teigė, kad šie mokėjimai laikytini autorizuotais, nes Mokėjimo kortelė inicijuojant Ginčijamus mokėjimus buvo pareiškėjos žinioje, o prie *Apple Pay* sistemos pridėta suvedus į pareiškėjos mobilųjį telefoną SMS žinute atsiųstą vienkartinį saugos kodą.

Vis dėlto, įvertinus pareiškėjos paaiškinimus apie Ginčijamų mokėjimų atlikimo aplinkybes ir iš banko vidaus sistemų surinktus duomenis, negalima daryti išvados, kad šie mokėjimai buvo inicijuoti ir patvirtinti pačios pareiškėjos, t. y. su jos žinia ir sutikimu.

Nors, ginčo bylos duomenimis, pareiškėjos Mokėjimo kortelė prie *Apple Pay* sistemos naujame įrenginyje galėjo būti pridėta suvedant ne tik šios kortelės duomenis (kortelės numerį, CVC kodą), bet ir banko į pareiškėjos mobilųjį telefoną SMS žinute atsiųstą vienkartinį saugos kodą, nustatyti ir banko neginčijami duomenys leidžia pagrįstai abejoti, ar mokėjimo priemonė, kuria atlikti Ginčijami mokėjimai, buvo tik pareiškėjos žinioje. Pareiškėjos nurodytomis[2] ir banko neginčijamomis aplinkybėmis, pareiškėjai Ginčijamų mokėjimų dieną paskambino banko darbuotoju prisistatęs asmuo, kurio telefono numeris pareiškėjos telefono ekrane buvo rodomas kaip banko telefono numeris ir kuris galėjo žinoti dieną prieš tai pareiškėjos suklastotoje interneto svetainėje atskleistus konfidencialius Mokėjimo kortelės duomenis, ir paprašė pareiškėjos papildomai atskleisti SMS žinute gautą vienkartinį saugos kodą, trečiojo asmens tariamai nurodytą kaip skirtą apsaugoti pareiškėjos Mokėjimo kortelės sąskaitoje esančias lėšas ir pašalinti pareiškėjos Mokėjimo kortelę iš *Apple Pay* atsiskaitymo metodo.

Dėl to, pačiai pareiškėjai neigiant Ginčijamų mokėjimų autorizavimo aplinkybę ir esant pagrįstų duomenų apie įvykusį sukčiavimo atvejį – taigi, kad pareiškėjos mokėjimo priemone ir jos personalizuotais saugumo duomenimis, be pareiškėjos žinios ir nesant jos valios, galėjo neteisėtai pasinaudoti tretieji asmenys, negalima daryti išvados, kad pareiškėjos Mokėjimo kortele atlikti Ginčijami mokėjimai buvo jos autorizuoti, t. y. inicijuoti ir patvirtinti esant pačios pareiškėjos sutikimui, kaip tai suprantama Mokėjimų įstatymo 29 straipsnio 1 dalies kontekste. Atsižvelgdamas į tai Lietuvos bankas daro išvadą, kad Ginčijami mokėjimai laikytini neautorizuotais.

2. *Dėl neautorizuotų mokėjimo operacijų pasekmių ir pareiškėjos teisės į Ginčijamų mokėjimų sumos grąžinimą*

Pagal Mokėjimų įstatymo 38 straipsnio 1 dalį, joje nurodytomis sąlygomis ir tvarka mokėtojo mokėjimo paslaugų teikėjas privalo grąžinti mokėtojui neautorizuotos mokėjimo operacijos sumą. Mokėjimų įstatymo 39 straipsnis nustato šios taisyklės taikymo išimtis.

Vadovaujantis Mokėjimų įstatymo 39 straipsnio 3 dalimi, 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[3] nustatytų pareigų.

---

[2] Pareiškėja nurodytas aplinkybes apie trečiųjų asmenų veiksmus pagrindė pateikdama 2022 m. gruodžio 26-27 d. gautų SMS žinučių bei 2022 m. gruodžio 27 d. telefono skambučių sąrašo ekrano nuotraukomis.

[3] 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, kaip minėta, 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 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 mokėtojo sukčiavimo (nesąžiningumo arba tyčios) arba didelio neatsargumo įrodymų, t. y. jeigu pagal mokėjimo paslaugų teikėjo pateiktus įrodymus nustatoma, kad mokėtojas ne tik neįvykdo vienos ar kelių jam Mokėjimų įstatyme nustatytų pareigų, bet ir padaro tai elgdamasis nesąžiningai arba tyčia ar būdamas labai neatsargus (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. Bankas sprendimą nekompensuoti pareiškėjos nuostolių grindžia vertinimu, kad Ginčijami mokėjimai buvo autorizuoti tinkamai. Be to, bankas mano, kad pareiškėjos elgesiui būdingas ir didelis neatsargumas.

Tai reiškia, kad, atsižvelgiant į pirmiau minėtas Mokėjimų įstatymo nuostatas, siekiant įvertinti, ar bankas pagrįstai atsisako kompensuoti pareiškėjos nuostolius, susijusius su Ginčijamų mokėjimų įvykdymu, ir ar pareiškėjai galėtų būti taikoma Mokėjimų įstatymo 39 straipsnio 3 dalis, būtina nustatyti, ar pareiškėjos elgesys atskleidžiant tam tikrus personalizuotus mokėjimo priemonės (mokėjimo kortelės) požymius ir (ar) kiti veiksmai, dėl kurių galėjo būti įvykdyti Ginčijami mokėjimai, vertintini kaip didelis neatsargumas, dėl kurio visi jos reikalaujami atlyginti nuostoliai turėtų tekti pačiai pareiškėjai.

Pirmiau minėtame Mokėjimų įstatymo 34 straipsnyje nustatyta viena iš mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigų – naudotis mokėjimo priemone pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas. Panašias pareigas nustato banko ir pareiškėjos bendrąją sutartį sudarančių banko Privatiems klientams taikomų sąlygų 9 dalis, kurioje 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, išskyrus atvirosios bankininkystės paslaugų teikėją ar trečiosios šalies teikėją, besilaikantį teisės aktų reikalavimų<...>"

Taigi, aptartos privatiems klientams taikomų sąlygų nuostatos aiškiai nustato, kad už tapatybės priemonės personalizuotų saugumo duomenų konfidencialumą yra atsakingas mokėtojas, šiuo atveju – pareiškėja. Atsižvelgiant į tai, manytina, kad pareiškėjos elgesys būtų laikomas atitinkančiu mokėjimo priemonės išdavimą ir naudojimą reglamentuojančio susitarimo sąlygas, jei būtų nustatyta, kad ji ėmėsi adekvačių veiksmų (arba nuo tam tikrų veiksmų susilaikė), kad būtų tinkamai užtikrintas banko išduotų mokėjimo priemonių personalizuotų saugumo duomenų, sudarančių sąlygas inicijuoti ir tvirtinti mokėjimus, konfidencialumas.

Vadovaujantis ginčo byloje esančiais banko vidaus sistemų duomenimis, pareiškėjos Ginčijami mokėjimai buvo įvykdyti Mokėjimo kortele, panaudojant *Apple Pay* mokėjimo metodą. Bankas paaiškino, kad banko išduota mokėjimo kortelė gali būti pridėta (angl. *tokenized*) prie bet kokio įrenginio, turinčio *Apple Pay* (*Google Pay*, *Garmin Pay* ar kt.) funkciją (telefono, išmaniosios apyrankės, laikrodžio, planšetės ir kita) ir šis įrenginys neturi (neprivalo) būti susietas su banke atidaryta asmenine mokėjimo sąskaita ar turėti banko mobiliosios programėlės. Banko teigimu, kad būtų galima atsiskaityti naudojant *Apple Pay* mokėjimo metodą, būtina mokėjimo kortelę pridėti prie *Apple Pay* sistemos. Mokėjimo kortelei prie *Apple Pay* sistemos pridėti taikoma saugesnio autentiškumo patvirtinimo procedūra, kurios metu reikia ne tik pateikti mokėjimo kortelės duomenis, bet ir suvesti vienkartinį saugos kodą[4], kuris, pagal banko pateiktus įrodymus, šiuo atveju ir buvo suvestas. Kaip paaiškino bankas, be pareiškėjos telefono numeriu išsiųsto vienkartinio saugos kodo suvedimo, pareiškėjos Mokėjimo kortelės pridėjimas prie *Apple Pay* nebūtų buvęs patvirtintas ir atsiskaitymas su *Apple Pay* būtų

[4] Pagal *Apple Pay* sąlygas, vienkartinis saugos kodas SMS žinute banko kliento telefono numeriu yra siunčiamas tik tuomet, kai suvedami teisingi mokėjimo kortelės, kurią siekiama pridėti prie *Apple Pay* įrenginio, duomenys.

buvęs neįmanomas. Įvedus neteisingą saugos kodą, visas procesas yra pradedamas iš naujo, tai yra vėl prašoma įvesti banko kortelės duomenis, ši informacija perduodama bankui, ją patvirtinus yra išsiunčiamas naujas vienkartinis saugos kodas SMS žinute. Banko pateiktais duomenimis, bandant pridėti pareiškėjos Mokėjimo kortelę prie *Apple Pay* mokėjimo metodo, pareiškėjai šiuo atveju buvo išsiųstos trys SMS žinutės su standartiniu tekstu ir vienkartiniu saugos kodu ir vienas iš šių kodų buvo suvestas, pridedant Mokėjimo kortelę prie *Apple Pay* mokėjimo metodo.

Pareiškėja neneigia prieš Ginčijamų mokėjimų įvykdymą tretiesiems asmenims atskleidusi SMS žinute gautą vienkartinį saugos kodą bei savo Mokėjimo kortelės duomenis. Pareiškėja, pateikdama paaiškinimus dėl Ginčijamų mokėjimų įvykdymo aplinkybių ir kartu dėl bankui keliamo reikalavimo pagrįstumo, nurodė, kad dieną prieš Ginčijamų mokėjimų įvykdymą gavo SMS žinutę iš „Royal Mail", kurioje buvo nurodyta, kad, nepavykus pristatyti siuntos, pareiškėja turi pasirinkti naują pristatymo laiką. Pareiškėja paspaudė SMS žinutėje pateiktą nuorodą ir atsidariusiame interneto puslapyje suvedė savo Mokėjimo kortelės duomenis, kad sumokėtų 2 GBP už tariamą pakartotinį siuntinio pristatymą į namus. Kitą dieną pareiškėja teigia supratusi, kad tai buvo apgavystė, ir tą pačią dieną, t. y. 2022 m. gruodžio 27 d., sulaukė skambučio iš tariamo „Revolut" darbuotojo, kuris pareiškėją informavo, kad jos Mokėjimo kortelė buvo galimai neteisėtai pridėta prie *Apple Pay*. Pareiškėja teigia trečiųjų asmenų buvusi informuota, kad, norėdama apsaugoti savo sąskaitą, pareiškėja turi nurodyti skambinančiam asmeniui SMS žinute gautą vienkartinį kodą.

Pareiškėja kreipimesi pažymi, kad jai skambinusio asmens, prisistačiusio banko darbuotoju (t. y. sukčiaus), telefono numerį jos telefonas identifikavo kaip banko telefono numerį, todėl šio asmens nurodymai nesuteikė pagrindo pareiškėjai suabejoti jo patikimumu[5]. Pareiškėja, kaip minėta, pripažįsta skambinančiam asmeniui (sukčiui) atskleidusi prašomą informaciją, šie jos veiksmai lėmė tai, kad pareiškėjos Mokėjimo kortelė buvo pridėta prie *Apple Pay* įrenginio, o juo vėliau atlikti ir Ginčijami mokėjimai.

Išanalizavęs ginčo byloje esančius duomenis ir kitas nustatytas aplinkybes, net ir įvertinęs tai, kad trečiųjų asmenų (sukčių) veiksmai, išviliojant pareiškėjos Mokėjimo kortelės duomenis ir apsimetant banko darbuotoju, iš tiesų galėjo sukurti klaidinantį pirminį įspūdį, Lietuvos bankas mano, kad pareiškėjos elgesys negali būti vertinamas kaip atsargus ir apdairus ar tik neatsargus.

Kaip nustatyta, pridedant pareiškėjos Mokėjimo kortelę prie *Apple Pay* sistemos naujame įrenginyje, turėjo būti suvesti teisingi šios Mokėjimo kortelės duomenys (įskaitant mokėjimo kortelės saugos kodą CVV) ir vienkartinis saugos kodas, kuris, banko Lietuvos bankui pateiktais duomenimis, buvo išsiųstas SMS žinute pareiškėjos telefono numeriu. Ginčo bylos duomenimis, kartu su vienkartiniu saugos kodu pareiškėjai SMS žinutėje buvo nurodyta šio kodo paskirtis ir perspėjimas jo neperduoti tretiesiems asmenims (standartinis siunčiamos SMS žinutės tekstas lietuvių kalba: „Šis kodas bus naudojamas jūsų kortelei pridėti prie kito Apple Pay įrenginio. Niekur jo neįveskite, nebent norite pridėti savo kortelę prie naujo įrenginio. Nesidalinkite šiuo kodu su niekuo, net jei jie teigia esantys iš Revolut. „Revolut" patvirtinimo kodas, skirtas „Apple Pay": xxxxxx")[6]. Suvedus gautą vienkartinį saugos kodą, Mokėjimo kortelės pridėjimas buvo patvirtintas, o atsiskaitymo *Apple Pay* paslauga aktyvuota – ja naudojantis ir inicijuoti bei patvirtinti visi Ginčijami mokėjimai. Svarbu ir tai, kad minėta SMS žinutė su vienkartiniu saugos kodu ir perspėjimu šio kodo niekam neatskleisti pareiškėjai iki jos Mokėjimo kortelės faktinio pridėjimo prie *Apple Pay* įrenginio buvo išsiųsta tris kartus (taigi, iš viso trys skirtingos žinutės su trimis skirtingais vienkartiniais saugaus kodais), tačiau perspėjimo niekam žinutėje nurodyto vienkartinio kodo neatskleisti pareiškėja nepamatė iki jo perskaitymo (atskleidimo) trečiajam asmeniui, t. y. jau po to, kai pareiškėja buvo atskleidusi žinutėje nurodytą vienkartinį saugos kodą. Pareiškėjos teigimu, perskaičiusi telefonu skambinusiam asmeniui, tariamam banko darbuotojui, vieną iš SMS žinute gautų vienkartinių saugos kodų, ji pamatė ir žinutėje pateiktą perspėjimą, tuomet suprato buvusi apgauta,

[5] Bankas paaiškino, kad šiuo atveju pareiškėja gavo SMS žinutę iš nežinomo numerio, o vėliau skambučio iš sukčių, kurie pasitelkę technologijas, paslepia (užmaskuoja) skambučius ir žinutes taip, kad atrodytų, jog skambina ar rašo tikrasis asmuo, šiuo atveju – „Royal Mail" ir (ar) bankas (angl. spoofing). *Spoofing* – tai nežinomo šaltinio pranešimų maskavimas kaip žinomo, patikimo šaltinio pranešimų. Sukčiavimas gali būti taikomas el. laiškams, telefono skambučiams ir svetainėms. Nagrinėjamo ginčo atveju, sukčiai savo telefono numerį užmaskavo banko numeriu, taip priversdami pareiškėją manyti, kad su ja iš tiesų susisiekė bankas.

[6] Tekstas anglų k.: „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".

išsigando ir išjungė savo telefoną. Po poros minučių įjungusi telefoną pareiškėja teigia pamačiusi vėl skambinant tą patį telefono numerį, tačiau į šį skambutį neatsiliepė. Prisijungusi prie savo mobiliosios programėlės, pamatė Mokėjimo kortele atliktus Ginčijamus mokėjimus ir bandė juos atšaukti, tačiau to padaryti negalėjo, todėl nedelsdama susisiekė su banku.

Vis dėlto, įvertinus pirmiau cituotą SMS žinutės su vienkartiniu saugos kodu tekstą, manytina, kad informacijos, kokiam tikslui skirtas šis pareiškėjai SMS žinute atsiųstas kodas, pareiškėja galėjo nematyti tik dėl to, kad buvo itin neatidi. Taigi, pareiškėja, neperskaičiusi žinutės teksto, pasitikėjo nepažįstamų jai skambinusių asmenų nurodymais ir atskleidė jiems šį kodą, nors, kaip minėta, tokios SMS žinutės su vienkartiniu saugos kodu ir perspėjimu jo neatskleisti tretiesiems asmenims pareiškėjai buvo siųstos net tris kartus 8 minučių laikotarpiu[7]. Tad nors skambinantis asmuo galėjo pasitelkti socialinės inžinerijos metodus ir sukelti baimę ir poreikį veikti neatidėliojant tam, kad pareiškėja tariamai apsaugotų savo Mokėjimo kortelę nuo pridėjimo prie *Apple Pay* sistemos ar ją pašalintų iš *Apple Pay* įrenginio, vis dėlto manytina, kad pareiškėja turėjo pakankamai laiko perskaityti tris kartus gautose SMS žinutėse nurodytus įspėjimus ir priimti labiau apgalvotus ir apdairius sprendimus.

Be to, svarbu ir tai, kad dieną prieš Ginčijamų mokėjimų įvykdymą pareiškėja, kaip teigia pati, buvo apgauta sukčių: paspaudė SMS žinutėje pateiktą nuorodą, tikėtina, suklastotoje siuntų bendrovės „Royal Mail" interneto svetainėje suvedė savo Mokėjimo kortelės duomenis, tačiau, net ir supratusi, kad buvo apgauta ir atskleidė savo mokėjimo priemonės personalizuotus saugumo duomenis tretiesiems asmenims, apie tai savo mokėjimo paslaugų teikėjui – bankui, nepranešė ir (ar) kitų veiksmų, kad apsaugotų savo mokėjimo priemonę nuo neteisėto panaudojimo, nesiėmė arba tokių duomenų Lietuvos bankui nepateikė, todėl pažeidė Mokėjimų įstatymo 34 straipsnio 2 dalies ir banko Privatiems klientams taikomų sąlygų 9 dalies reikalavimus. Tokie itin neapdairūs veiksmai – tiek Mokėjimo kortelės duomenų atskleidimas, tiek vėliau atskleistas vienkartinis saugos kodas, įgalino trečiuosius asmenis susieti pareiškėjos Mokėjimo kortelę su *Apple Pay* mokėjimo metodu, o vėliu ir įvykdyti Ginčijamus mokėjimus.

Tai reiškia, kad Ginčijamus mokėjimus tretieji asmenys be pareiškėjos žinios galėjo atlikti tik dėl to, kad pareiškėja, būdama labai neatsargi, netinkamai vykdė Mokėjimų įstatyme (34 straipsnis) ir Privatiems klientams taikomose sąlygose įtvirtintus mokėjimo kortelės saugaus naudojimo reikalavimus. Taigi, labiausiai tikėtina, kad būtent pareiškėja dėl didelio neatsargumo neišsaugojo jos vardu išduotos mokėjimo kortelės duomenų konfidencialumo, t. y. nesiėmė tų saugumo priemonių, kurių privalėjo imtis, kad būtų tinkamai apsaugoti jai suteiktos mokėjimo kortelės duomenys, ir tretiesiems asmenims suteikė (nurodė) vienkartinį saugos kodą, kurį gavo į jai priklausantį telefono numerį trumpąją SMS žinute, nors ta pačia SMS žinute buvo papildomai įspėta apie būtinybę saugoti ir niekam neatskleisti atsiųsto saugos kodo.

Konstatavus, kad pareiškėja, nesilaikydama jai, kaip mokėtojai, Mokėjimų įstatyme ir bendrojoje sutartyje su banku nustatytų pareigų, susijusių su išduotomis mokėjimo priemonėmis, elgėsi labai neatsargiai, 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.

Atsižvelgiant į tai, Lietuvos banko vertinimu, bankas neprivalo grąžinti (kompensuoti) pareiškėjai neautorizuotų Ginčijamų mokėjimų lėšų ir pareiškėjos reikalavimas, kad bankas grąžintų pareiškėjai Ginčijamų mokėjimų lėšas - 2 590 GBP, atmestinas kaip nepagrįstas.

3. Dėl banko teikiamų paslaugų saugumo

Norėdama pagrįsti bankui keliamą reikalavimą, pareiškėja kreipimesi taip pat teigia, kad bankas netinkamai įvykdė savo pareigą apsaugoti jos lėšas

Pažymėtina, kad finansų rinkos dalyviai, tarp jų ir bankas, teikdami finansines paslaugas, turi veikti profesionaliai ir skaidriai. Bankui, kaip profesionaliam verslininkui ir savo srities specialistui, yra keliami aukštesni profesionalumo, atidumo ir rūpestingumo standartai, todėl turėdamas specifinių finansinių paslaugų teikimo srities žinių, bankas turėtų dėti visas reikiamas bei protingai įmanomas pastangas (įskaitant ir tinkamų prevencinių priemonių, teikiant mokėjimo paslaugas, įdiegimą) tam, kad klientai būtų kaip įmanoma labiau apsaugoti nuo neautorizuotų ir (ar) nesąžiningų mokėjimo operacijų ir turėtų visas galimybes ginčijamų

[7] Banko vidaus sistemų duomenys apie pareiškėjos telefono numeriu siųstas SMS žinutes su vienkartiniu saugos kodu (2022 m. gruodžio 27 d. 15:34 – 15:42 val. (vietos laiku)).

mokėjimo operacijų lėšas bandyti susigrąžinti, ypač sukčiavimų elektroninėje erdvėje atvejais[8].

Bankas pateikdamas paaiškinimus dėl teikiamų mokėjimo paslaugų saugumo, pažymėjo, kad, siekiant užtikrinti mokėjimo kortelės duomenų saugumą, vienkartinis saugos kodas visais atvejais yra siunčiamas tuo telefono numeriu, kuris yra susietas su mokėjimo kortele, t. y. bankui, kuris išdavė mokėjimo kortelę, žinomu numeriu, nurodytu banko ir mokėjimo kortelės savininko sudarytoje sutartyje. Būtent šis saugumo kriterijus lemia tai, kad pridedant mokėjimo kortelę prie *Apple Pay* negalima ir neįmanoma pakeisti telefono numerio, kuriuo bus siunčiamas saugos kodas, šis kodas visais atvejais yra siunčiamas banko turimu telefono numeriu.

Nagrinėjamo ginčo atveju, pridedant pareiškėjos Mokėjimo kortelę prie *Apple Pay* įrenginio, buvo suvesti teisingi Mokėjimo kortelės duomenys ir suvestas teisingas vienkartinis saugos kodas, kuris buvo išsiųstas SMS žinute pareiškėjos telefono numeriu. Bankas, atlikęs tyrimą dėl pareiškėjos Ginčijamų mokėjimų, nenustatė jokių sąskaitos perėmimo ženklų, nagrinėjamam ginčui aktualiu laikotarpiu į banko vidaus sistemas taip pat nebuvo įsilaužta ir (ar) jos nebuvo paveiktos techninių trikdžių, dėl kurių pareiškėjos Mokėjimo kortelės duomenys ir (ar) pareiškėjai siųstas vienkartinis saugos kodas galėjo tapti žinomi tretiesiems asmenims.

Kaip minėta, Lietuvos bankas nagrinėdamas ginčus neatlieka patikrinimų tam, kad nustatytų, ar nebuvo pažeisti finansų įstaigų veiklai keliami teisės aktų reikalavimai. Lietuvos bankas remiasi ginčo šalių pateiktais konkrečiais įrodymais, kurių pagrindu priima sprendimą. Atsižvelgiant į tai, darytina išvada, kad ginčo byloje nėra jokių duomenų, galinčių patvirtinti pareiškėjos nurodytą aplinkybę, kad bankas nesiėmė reikiamų veiksmų, kad apsaugotų pareiškėjos banko sąskaitose esančias lėšas, o įvykdydamas Ginčijamus mokėjimus bankas būtų pažeidęs finansų rinką reglamentuojančių teisės aktų reikalavimus. Priešingai, nustatytais duomenimis, pareiškėjos Mokėjimo kortelės pridėjimą prie *Apple Pay* įrenginio ir vėliau Ginčijamų mokėjimų įvykdymą lėmė pačios pareiškėjos itin neatsargūs veiksmais, naudojantis savo mokėjimo priemone.

Verta atkreipti dėmesį ir į tai, kad faktas, jog, vykdydama trečiųjų asmenų apgaulingus nurodymus, pareiškėja sudarė sąlygas savo Mokėjimo kortelę pridėti prie *Apple Pay* mokėjimo sistemos ir įvykdyti Ginčijamus mokėjimus, savaime nereiškia, kad bankas nesilaikė teisės aktų reikalavimų, susijusių su lėšų mokėjimo kortelės sąskaitoje saugumo užtikrinimu. Aplinkybė, kad Ginčijami mokėjimai buvo įvykdyti dėl trečiųjų asmenų apgaulingų ir neteisėtų veiksmų, paaiškėjo jau vėliau, t. y. po Ginčijamų mokėjimų įvykdymo, apie tai pačiai pareiškėjai informavus banką.

Atsižvelgiant į tai, nėra pagrindo teigti, kad bankas būtų netinkamai įvykdęs savo pareigą užtikrinti pareiškėjos Mokėjimo kortelės sąskaitoje esančių lėšų saugumą.

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

[8] Tai, kad verslininkui, šiuo atveju - ir bankui, kaip ir bet kuriam kitam savo srities profesionalui, teikiančiam paslaugas, teisės aktai nustato aukštesnį profesionalo teisėto elgesio standartą, taigi, kad jam taikomi aukštesni profesionalumo, atidumo ir rūpestingumo standartai, savo praktikoje ne kartą yra pabrėžęs ir kasacinis teismas. Pavyzdžiui, Lietuvos Aukščiausiojo Teismo 2008 m. vasario 28 d. nutartis civilinėje byloje Nr. 3K-3-112/2008; 2010 m. kovo 1 d. nutartis civilinėje byloje Nr. 3K-3-69/2010; 2018 m. spalio 12 d. nutartis civilinėje byloje Nr. e3K-3-60-969/2018.