LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

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

2022 m. rugsėjo 7 d. Nr. 429-435
Vilnius

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

N u s t a t y t a:

2022 m. balandžio 27–28 d. banko pareiškėjai išduota *Mastercard* mokėjimo kortele (toliau – Mokėjimo kortelė) buvo inicijuotos 5 mokėjimo operacijos, kurių bendra vertė 745,31 Eur: 1) 2022 m. balandžio 27 d. NOK 547,62 vertės mokėjimas naudos gavėjui Z. Z.; 2) 2022 m. balandžio 27 d. NOK 1 529,37 vertės mokėjimas naudos gavėjui Z. Z.; 3) 2022 m. balandžio 28 d. NOK 1 254,42 vertės mokėjimas naudos gavėjui Z. Z.; 4) 2022 m. balandžio 28 d. NOK 819,85 vertės mokėjimas naudos gavėjui Z. Z.; 5) 2022 m. balandžio 28 d. 340,50 EUR vertės mokėjimas naudos gavėjui C. C. (toliau – Ginčijami mokėjimai).

2022 m. balandžio 28 d. pareiškėja pateikė prašymą bankui dėl pinigų grąžinimo procedūros pagal tarptautinės mokėjimo kortelių organizacijos *Mastercard* taisykles inicijavimo.

2022 m. balandžio 29 d. po atlikto vidinio tyrimo bankas informavo pareiškėją, kad nesąžiningos veiklos pėdsakų jos sąskaitoje nenustatyta, todėl bankas neinicijuos lėšų grąžinimo procedūros dėl pareiškėjos Ginčijamų mokėjimų.

2022 m. balandžio 30 d. pareiškėja susisiekė su banko klientų aptarnavimo specialistais ir pakarotinai informavo banką, kad jos Mokėjimo kortelė galėjo būti neteisėtai panaudota Ginčijamiems mokėjimams atlikti, ir paprašė Ginčijamų mokėjimų lėšas kompensuoti. 2022 m. gegužės 2 d. ir 2022 m. gegužės 18 d. pareiškėja taip pat pateikė pretenzijas bankui dėl atsisakymo inicijuoti lėšų grąžinimo procedūrą dėl Ginčijamų mokėjimų ir (ar) kitu būdu kompensuoti jos su Ginčijamų mokėjimų įvykdymu susijusių nuostolių.

2022 m. gegužės 6 d. bankas pateikė atsakymą pareiškėjai ir informavo, kad banko sprendimas nekompensuoti pareiškėjos nuostolių dėl Ginčijamų mokėjimų įvykdymo, taip pat ir sprendimas neinicijuoti lėšų grąžinimo procedūros yra galutinis ir nebus keičiamas.

Pareiškėja nesutinka su banko sprendimu. Kreipimesi pareiškėja teigia, kad savo sutikimo atlikti Ginčijamus mokėjimus ji nedavė ir Ginčijamų mokėjimų, kaip neautorizuotų mokėjimo operacijų, sumos turi būtų grąžintos į pareiškėjos sąskaitą banke.

Bankas, pagrįsdamas savo poziciją nekompensuoti pareiškėjos nuostolių dėl Ginčijamų mokėjimų įvykdymo, nurodo, kad Ginčijami mokėjimai buvo atlikti ir autorizuoti panaudojant bekontaktį mokėjimo (atsiskaitymo) metodą *Apple Pay*. Bankas nurodo, kad, atliekant tyrimą dėl pareiškėjos Ginčijamų mokėjimų ir patikrinus Mokėjimo kortelės įvykių registrą, buvo pastebėta, kad 2022 m. balandžio 27 d. Mokėjimo kortelė buvo pirmą kartą susieta su *Apple Pay* pareiškėjai nepriklausančiame (pareiškėjos įprastai iki Ginčijamų mokėjimų įvykdymo nenaudojamame) mobiliajame įrenginyje pavadinimu *iPhone de* (*duomenys neskelbtini*). Atsižvelgdami į tai, banko specializuotos pinigų grąžinimo komandos nariai konstatavo, jog visi Ginčijami mokėjimai buvo atlikti su *Apple Pay* iš to paties pašalinio *iPhone de* (*duomenys neskelbtini*) mobiliojo įrenginio, kuris, kaip *Apple Pay* mokėjimo įrenginys, banko turimais duomenimis, buvo patvirtintas pareiškėjos. Bankas pažymėjo, kad mokėjimo kortelės turėtojas,

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

norėdamas prie *Apple Pay* sistemos pridėti mokėjimo kortelę, kuria siekia atlikti mokėjimo operacijas, turi suvesti kortelės duomenis (kortelės numerį, saugos kodą (CVV)) ir papildomai patvirtinti mokėjimo kortelės pridėjimą prie *Apple Pay* sistemos įvesdamas vienkartinį saugos kodą, kurį gauna SMS žinute. Žinutė su vienkartiniu saugos kodu visais atvejais siunčiama į telefono numerį, kuris nurodomas ir autorizuojamas vartotojui sudarant sutartį su banku.

Bankas atkreipia dėmesį į tai, kad pati pareiškėja patvirtino, kad jos Mokėjimo kortelė buvo jos žinioje ir niekam kitam ji jos nebuvo perdavusi. Be to, banko teigimu, net jeigu mokėjimo kortelės duomenys būtų atskleisti ar įgyti be mokėjimo kortelės savininko žinios, beveik neįmanoma, kad trečioji šalis be kortelės savininko žinios galėtų gauti ir vienkartinį saugos kodą, kuris šiuo atveju SMS žinute buvo išsiųstas į pareiškėjos telefono numerį. Banko vertinimu, atsižvelgiant į tai, kad Ginčijamų mokėjimų autentiškumo patvirtinimo procedūra buvo atlikta tinkamai, tikėtina, jog net jei šiuos mokėjimus inicijavo ne pati pareiškėja, būtent dėl jos netinkamo elgesio jos Mokėjimo kortelės duomenys ir SMS žinute gautas vienkartinis saugos kodas buvo atskleisti tretiesiems asmenims. Bankas mano, kad pareiškėja netinkamai vykdė jai, kaip mokėtojai, nustatytą pareigą gavus mokėjimo priemonę imtis veiksmų, kad būtų apsaugoti jos personalizuoti saugumo duomenys, o sužinojus apie mokėjimo priemonės praradimą, vagystę arba neteisėtą pasisavinimą ar neautorizuotą jos naudojimą, nedelsiant apie tai pranešti bankui kaip pareiškėjos mokėjimo paslaugų teikėjui.

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. 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 745,31 Eur, sumą. Pareiškėja teigia nedavusi sutikimo atlikti Ginčijamus mokėjimus, neigia juos autorizavusi ir (ar) pridėjusi savo Mokėjimo kortelę prie *Apple Pay* sistemos iš naujo įrenginio. Bankas, remdamasis vidaus sistemų duomenimis, pažymi, kad pareiškėjos Mokėjimo kortelė prie *Apple Pay* sistemos buvo pridėta naudojant Mokėjimo kortelės duomenis (kortelės numerį, CVV kodą) ir pridėjimą patvirtinant banko į sutartyje nurodytą telefono numerį išsiųstoje žinutėje pateiktu vienkartiniu saugos kodu. Bankas mano, kad Ginčijamus mokėjimus autorizavo pati pareiškėja arba pareiškėja dėl didelio neatsargumo atskleidė tretiesiems asmenims savo Mokėjimo kortelės duomenis ir vienkartinį saugos kodą, kuriais pasinaudoję tretieji asmenys įgijo galimybę inicijuoti Ginčijamus mokėjimus.

Siekiant išspręsti šį pareiškėjos ir banko ginčą, Lietuvos banko vertinimu, būtina nustatyti, ar Ginčijami mokėjimai laikytini autorizuotais ir ar bankas privalo grąžinti pareiškėjai Ginčijamų mokėjimų sumą.

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.

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. Šiuos veiksmus bankas laiko mokėtojo sutikimu atlikti mokėjimus iš banko sąskaitos[2]. Atsižvelgiant į tai, kad bendroji sutartis (ją sudarančios banko privatiems klientams taikomos sąlygos) nustato banko ir pareiškėjos tarpusavio santykius, ir 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.

Pagal banko kartu su atsiliepimu pateiktus vidaus sistemos duomenis, visi pareiškėjos Ginčijami mokėjimai atlikti tuo pačiu mobiliuoju įrenginiu („iPhone de (*duomenys neskelbtini*)"), 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. balandžio 27 d. Vadovaujantis aptartais banko vidaus sistemų duomenimis, pareiškėjai vienkartinis saugos kodas SMS žinute buvo išsiųstas (ir gautas) pareiškėjos telefono numeriu (+346 *** ** 675) 2022 m. balandžio 27 d. 16:49 UTC laiku, t. y. 23 sekundės iki Mokėjimo kortelės pridėjimo prie *Apple Pay* sistemos ne pareiškėjos naudojamame mobiliajame įrenginyje („iPhone de (*duomenys neskelbtini*)"). Tai reiškia, kad, pridedant minėtą mobilųjį įrenginį, kaip *Apple Pay* mokėjimo įrenginį, buvo panaudoti pareiškėjos Mokėjimo kortelės duomenys ir suvestas banko SMS žinute į pareiškėjos mobilųjį telefoną atsiųstas vienkartinis saugos kodas. Vis dėlto, sprendžiant, ar Ginčijami mokėjimai laikytini pareiškėjos autorizuotais, būtina pažymėti, kad ginčo byloje nėra jokių duomenų, kur ir kokią informaciją (duomenis) matydama ir žinodama pareiškėja galėjo suvesti savo Mokėjimo kortelės duomenis ir SMS žinute gautą vienkartinį saugos kodą. Ginčo byloje taip pat nėra jokių patikimų įrodymų, kad minėtus mokėjimo priemonių personalizuotus saugumo duomenis Mokėjimo kortelei prie *Apple Pay* sistemos naujame įrenginyje pridėti tikrai suvedė pati pareiškėja, o ne tretieji asmenys, galėję pareiškėjos mokėjimo priemonių personalizuotus saugumo duomenis sužinoti (išvilioti) neteisėtai.

Atsiliepime, net ir atsižvelgdamas į tai, kad Ginčijami mokėjimai buvo inicijuoti jų įvykdymo dieną naujame įrenginyje, prie *Apple* Pay sistemos pridėjus pareiškėjos Mokėjimo kortelę, bankas teigė, kad Ginčijami mokėjimai turi būti laikomi autorizuotais, nes Mokėjimo kortelė ir mobilusis įrenginys inicijuojant Ginčijamus mokėjimus buvo pareiškėjos žinioje, o tiek Mokėjimo kortelės pridėjimas prie *Apple* Pay sistemos, tiek vėliau ir patys Ginčijami mokėjimai buvo patvirtinti šalių bendrojoje sutartyje sutarta forma.

Įvertinus pareiškėjos paaiškinimus apie Ginčijamų mokėjimų atlikimo aplinkybes ir iš banko vidaus sistemų surinktus duomenis, vis dėlto negalima daryti pagrįstos 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 buvo pridėta suvedant ne tik šios kortelės duomenis (kortelės numerį, CVC kodą), bet ir banko į pareiškėjos mobilųjį telefoną SMS žinute atsiųstą vienkartinį saugos kodą, ginčo nagrinėjimo metu nustatyti duomenys leidžia pagrįstai abejoti, ar ši pareiškėjai banko išduota mokėjimo priemonė, kuria atlikti Ginčijami mokėjimai, buvo tik pareiškėjos žinioje. Dėl to, pačiai pareiškėjai neigiant Ginčijamų mokėjimų autorizavimo aplinkybę ir byloje nesant kitų įrodymų, patvirtinančių, kad Ginčijamus mokėjimus autorizavo pareiškėja, negalima daryti išvados, kad pareiškėjos mokėjimo priemone (kuri nustatytomis aplinkybėmis galėjo būti pasisavinta ir (ar) ja neteisėtai pasinaudota) 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 šiuo atveju pareiškėjos Ginčijami mokėjimai laikytini neautorizuotais.

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

Pagal Mokėjimų įstatymo 38 straipsnio 1 dalį, mokėtojo mokėjimo paslaugų teikėjas

[2] 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*.

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). Pagal Mokėjimų įstatymo 39 straipsnio 1 dalį, 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 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. jei 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. Kaip minėta, bankas sprendimą nekompensuoti pareiškėjos nuostolių grindžia aplinkybe, kad Ginčijami mokėjimai buvo autorizuoti tinkamai, t. y. pareiškėjos Mokėjimo kortelę, kuria šie mokėjimai atlikti, prie *Apple Pay* sistemos pridėjus taikant saugesnio autentiškumo patvirtinimo procedūrą, tačiau kartu nurodo, kad pareiškėjos elgesiui būdingas ir didelis neatsargumas. Tai reiškia, kad, atsižvelgiant į pirmiau minėtas Mokėjimų įstatymo nuostatas, taip pat ir į šiuos banko teiginius, 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 (banko išduotos 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 reglamentuojančias 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.

Pareiškėja, pateikdama paaiškinimus dėl Ginčijamų mokėjimų įvykdymo aplinkybių ir kartu dėl savo banko atžvilgiu keliamo reikalavimo pagrįstumo, nurodė, kad niekada niekam nėra atskleidusi savo mokėjimo priemonių personalizuotų saugumo duomenų ir niekada nebuvo praradusi savo Mokėjimo kortelės ir (ar) jos valdymo kontrolės. Ginčijami mokėjimai, pareiškėjos vertinimu, buvo inicijuoti ir įvykdyti dėl trečiųjų asmenų neteisėtų veiksmų.

Vadovaujantis ginčo byloje esančiais banko vidaus sistemų duomenimis, pareiškėjos Ginčijami mokėjimai buvo inicijuoti panaudojant *Apple Pay* mokėjimo nurodymo patvirtinimo metodą. Banko teigimu, kad būtų galima atsiskaityti naudojant *Apple Pay*, 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, o tai, banko pateiktais įrodymais, šiuo atveju ir buvo atlikta. Bankas nurodė, kad jokių techninių trikdžių atliekant Ginčijamus mokėjimus nebuvo neužfiksuota, taip pat nebuvo užfiksuota jokių trečiųjų asmenų įsilaužimo į pareiškėjos Mokėjimo kortelės sąskaitą banko programėlėje požymių.

Įrodymų pakankamumas civiliniame procese grindžiamas tikėtinumo taisykle (tikimybių pusiausvyros principas). 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].

Tad nors pareiškėja teigė, kad jokių savo mokėjimo priemonių personalizuotų saugumo duomenų ir (ar) kokių nors kitų savo duomenų niekam nėra atskleidusi, o Mokėjimo kortelės ir (ar) jos valdymo kontrolės niekada nebuvo praradusi, ginčo byloje nustatyta, kad pareiškėjos Mokėjimo kortelė prie *Apple Pay* sistemos naujame įrenginyje pridėta suvedus Mokėjimo kortelės numerį ir šios kortelės CVC kodą, taip pat būtent į pareiškėjos mobilųjį telefoną siųstą vienkartinį saugos kodą. Nesant kitų galimybių nustatyti ir (ar) nenustačius kitokias aplinkybes pagrindžiančių duomenų, kaip pareiškėjos mokėjimo priemonių personalizuoti saugumo duomenys be pačios pareiškėjos veiksmų galėjo tapti žinomi tretiesiems asmenims, kai, pareiškėjos teigimu, jos mobilusis telefonas ir (ar) Mokėjimo kortelė buvo jos žinioje, neginčijant konstatuotos aplinkybės, kad Ginčijami mokėjimai yra neautorizuoti ir jų įvykdyti savo valia pareiškėja nesiekė, labiau tikėtina, kad būtent pati pareiškėja, galbūt nesuprasdama atliekamų veiksmų reikšmės ir pasekmių, atskleidė tretiesiems asmenims visus duomenis, būtinus jos Mokėjimo kortelei pridėti prie *Apple Pay* sistemos naujame įrenginyje, iš kurio vėliau ir buvo inicijuoti visi Ginčijami mokėjimai.

Pareiškėjai nepateikus detalių paaiškinimų, kaip galėjo įvykti sukčiavimo ataka, dėl kurios iš jos sąskaitos banke įvykdyti Ginčijami mokėjimai, taip pat neigiant bet kokių su mokėjimo priemonėmis susijusių duomenų atskleidimą tretiesiems asmenims, net ir esant priešingas aplinkybes patvirtinantiems įrodymams, objektyviai neįmanoma tiksliai nustatyti visų tikrųjų Ginčijamų mokėjimų ir jų įvykdymą lėmusių aplinkybių. Kaip nustato Taisyklių 45 punktas, vartojimo ginčai Lietuvos banke nagrinėjami laikantis rungimosi principo – 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. Be to, pagal Taisyklių 43 punktą, Lietuvos bankas ginčą nagrinėja vertindamas ginčo šalių pateiktus rašytinius ir (ar) daiktinius įrodymus.

Vis dėlto, išanalizavęs ginčo byloje esančius duomenis ir kitas ginčo nagrinėjimo metu nustatytas aplinkybes, Lietuvos bankas mano, kad pareiškėjos elgesys negali būti vertinamas

[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.

kaip atsargus ir apdairus ar tik neatsargus. Kaip nustatyta, pridedant pareiškėjos Mokėjimo kortelę prie *Apple Pay* sistemos naujame įrenginyje, buvo 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. Kaip nurodė bankas atsiliepime, kartu su vienkartiniu saugos kodu pareiškėjai SMS žinutėje buvo nurodyta šio kodo paskirtis ir perspėjimas jo neperduoti tretiesiems asmenims (standartinis siunčiamos SMS žinutės tekstas anglų kalba: *Revolut verification code for Apple Pay: *******. Never share it with anyone, ever.*). Suvedus gautą saugos kodą, mokėjimo kortelės pridėjimas buvo patvirtintas, o atsiskaitymo *Apple Pay* paslauga aktyvuota – ja naudojantis ir inicijuoti bei patvirtinti visi Ginčijami mokėjimai.

Kaip nurodoma atsiliepime, be pareiškėjos telefono numeriu išsiųsto vienkartinio saugos kodo suvedimo į *Apple Pay* pareiškėjos Mokėjimo kortelės pridėjimas nebūtų buvęs patvirtintas ir atsiskaitymas su *Apple Pay* būtų buvęs neįmanomas: įvedus neteisingą saugos kodą, visas procesas pradedamas iš naujo, t. y. vėl prašoma suvesti mokėjimo kortelės duomenis, ši informacija perduodama mokėjimo paslaugų teikėjui, ją patvirtinus išsiunčiamas naujas vienkartinis saugos kodas SMS žinute. Įvertinus tai, kad pareiškėjos Mokėjimo kortelė ir mobilusis telefonas, kaip teigia pati pareiškėja, buvo jos žinioje, Mokėjimo kortelės duomenys ir, neabejotina, į pareiškėjos mobiluįį telefoną siųsta SMS žinute gautas vienkartinis saugos kodas tretiesiems asmenims galėjo tapti žinomi tik dėl to, kad pati pareiškėja, elgdamasi itin neapdairiai, šiuos duomenis atskleidė (nurodė) tretiesiems asmenims. Tai reiškia, kad Ginčijamus mokėjimus tretieji asmenys be pareiškėjos žinios galėjo atlikti tik dėl to, kad pareiškėja, būdama labai neatsargi, netinkamai vykdė Mokėjimų įstatymo (34 straipsnis) ir privatiems klientams taikomose sąlygose įtvirtintus mokėjimo kortelės saugaus naudojimo reikalavimus. 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. Dėl to, Lietuvos banko vertinimu, bankas neprivalo grąžinti (kompensuoti) pareiškėjai neautorizuotų Ginčijamų mokėjimų lėšų ir pareiškėjos reikalavimas rekomenduoti bankui kompensuoti pareiškėjai Ginčijamų mokėjimų lėšas atmestinas kaip nepagrįstas.

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