LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

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

2022 m. liepos 8 d. Nr. 429-294
Vilnius

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

N u s t a t y t a:

2022 m. kovo 4 d. pareiškėjai banko išduota mokėjimo kortele, naudojant *Apple Pay* mokėjimo nurodymo patvirtinimo metodą, įvykdytos penkios mokėjimo operacijos gavėjui *Mercuryo (*toliau – gavėjas), kurių bendra suma 5 050 Eur (toliau – ginčijami mokėjimai). Tą pačią dieną pareiškėja, naudodamasi banko mobiliąja programėle, susisiekė su banko klientų aptarnavimo komanda ir informavo, kad jos mokėjimo kortele galėjo būti neteisėtai atsiskaityta (atlikti ginčijami mokėjimai). Pareiškėjai patarta tiesiogiai susisiekti su paslaugos teikėju, kuriam buvo atlikti mokėjimai, siekiant atgauti pervestas sumas. Atsižvelgdami į pareiškėjos pateiktą informaciją banko klientų aptarnavimo specialistai paprašė užpildyti ir pateikti oficialų lėšų grąžinimo (angl. *chargeback*) prašymą, kuris leistų banko specialistų komandai išnagrinėti pretenziją dėl lėšų grąžinimo ir inicijuoti mokėjimo grąžinimo procedūrą tarptautinės mokėjimo kortelių organizacijos *Visa* nustatyta tvarka.

2022 m. kovo 4 d. pareiškėja užpildė ir bankui pateikė mokėjimo grąžinimo prašymą, taip pat užblokavo savo mokėjimo kortelę (*duomenys neskelbtini*), kuria buvo atlikti ginčijami mokėjimai.

Atlikęs tyrimą ir neradęs jokių apgaulingos veiklos požymių, bankas priėmė sprendimą atsisakyti grąžinti pareiškėjai ginčijamų mokėjimų sumą, įvertinęs, kad pati pareiškėja yra atsakinga už atliktus ginčijamus mokėjimus.

Pareiškėja nesutiko su banko sprendimu nekompensuoti jos nuostolių dėl ginčijamų mokėjimų įvykdymo ir kreipėsi į Lietuvos banką. Kreipimesi pareiškėja nurodė, kad 2022 m. kovo 4 d. tapo sukčiavimo atakos auka ir dėl to patyrė nuostolių – iš jos sąskaitos banke buvo nuskaičiuota 5 050 Eur suma. Pareiškėjos vertinimu, bankas nedėjo reikiamų pastangų, kad įvertintų jos situaciją, todėl sprendimas nekompensuoti nuostolių dėl įvykdytų ginčijamų mokėjimų, kurių sumas neteisėtai pasisavino sukčiai, yra nepagrįstas. Pareiškėja prašė rekomenduoti bankui grąžinti ginčijamų mokėjimų sumą.

Bankas nesutinka tenkinti pareiškėjos reikalavimo. Remdamasis vidaus sistemos duomenis bankas paaiškino, kad ginčijami mokėjimai atlikti naudojant *Apple Pay* mokėjimo nurodymo patvirtinimo metodą – prie *Apple Pay* sistemos buvo pridėta pareiškėjos mokėjimo kortelė. Bankas pažymėjo, kad mokėjimo kortelės turėtojas, 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.

Banko teigimu, pareiškėja patvirtino, kad jos mokėjimo kortelė buvo jos žinioje ir niekam kitam ji jos nebuvo perdavusi. Be to, net jeigu mokėjimo kortelės duomenys būtų atskleisti ar įgyti be mokėjimo kortelės savininko žinios, beveik neįmanoma, kad trečioji šalis

[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.

be kortelės savininko žinios galėtų gauti ir vienkartinį saugos kodą, kuris šiuo atveju SMS žinute buvo išsiųstas į pareiškėjos telefono numerį. Banko manymu, 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 atskleistas tretiesiems asmenims. Banko vertinimu, 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.

Bankas pažymėjo, kad pareiškėjos mokėjimo kortelė prie *Apple Pay* sistemos buvo pridėta 16.33 val. ir pirmasis ginčijamas mokėjimas atliktas 16.54 val. Taigi jeigu *Apple Pay* patvirtinimo kodo informacija nebūtų buvusi atskleista trečiajai šaliai, pridėti kortelės prie *Apple Pay*, esančios kitame neatpažintame įrenginyje, būtų buvę faktiškai neįmanoma. Banko teigimu, jo vidaus sistemų duomenys neužfiksavo mėginimo prie pareiškėjos sąskaitos ar programėlės paskyros jungtis iš naujo ir (ar) pareiškėjos neautorizuoto įrenginio.

Kadangi, banko turimais duomenimis, mokėjimo kortelė buvo pridėta prie *Apple Pay* sistemos ir suvestas vienkartinis SMS žinute į pareiškėjos telefono numerį gautas saugos kodas, bankas nurodė negalintis tenkinti pareiškėjos prašymo grąžinti ginčijamų mokėjimų lėšas ir prašė šį pareiškėjos reikalavimą laikyti nepagrįstu.

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 (toliau – Taisyklės) 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.

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 5 050 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. Lėšos iš jos mokėjimo kortelės sąskaitos buvo nurašytos dėl to, kad tretieji asmenys galėjo pasisavinti jos mokėjimo kortelės duomenis, todėl bankas turi jai grąžinti ginčijamų mokėjimų sumą. Bankas teigia, kad ginčijami mokėjimai buvo įvykdyti naudojant *Apple Pay* mokėjimo nurodymo patvirtinimo metodą. Banko vidaus sistemų duomenys patvirtina, kad pareiškėjos mokėjimo kortelė buvo pridėta prie *Apple Pay* sistemos naudojant mokėjimo kortelės duomenis (kortelės numerį, CVV kodą) ir pridėjimą patvirtinant banko į sutartyje nurodytą telefono numerį išsiųstoje žinutėje pateiktu vienkartiniu saugos kodu. Banko vertinimu, ginčijamus mokėjimus autorizavo pati pareiškėja arba dėl didelio neatsargumo atskleidė tretiesiems asmenims mokėjimo kortelės duomenis ir vienkartinį saugos kodą. Dėl to tretieji asmenys galėjo įgyti galimybę inicijuoti ginčijamus mokėjimus naudodamiesi pareiškėjos dėl didelio neatsargumo atskleistais duomenimis.

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.

Banko kartu su atsiliepimu pateiktais vidaus sistemos duomenimis, visi pareiškėjos ginčijami mokėjimai atlikti tuo pačiu mobiliuoju įrenginiu (įrenginio pavadinimas matomas banko sistemose - (*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. kovo 4 d. 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 būtina pažymėti, kad ginčo byloje nėra jokių duomenų, kur ir kokią informaciją (duomenis) matydama ir žinodama pareiškėja galėjo suvesti 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 šie mokėjimai negalėjo būti atlikti sukčių, nes buvo inicijuoti naudojant *Apple Pay* mokėjimo nurodymo patvirtinimo metodą, o mokėjimo kortelė ir mobilusis įrenginys inicijuojant mokėjimo operacijas buvo pareiškėjos žinioje. Bankas nepaaiškino ir niekaip nepagrindė, kodėl vertina, kad ginčijami mokėjimai naudojant *Apple Pay* mokėjimo nurodymo patvirtinimo metodą buvo įvykdyti ne naujame, bet pareiškėjai priklausančiame ir jos žinioje esančiame mobiliajame įrenginyje, nors pati pareiškėja neigia 2022 m. kovo 4 d. ar kitu metu pridėjusi savo mokėjimo kortelę prie *Apple Pay* sistemos naujame įrenginyje.

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 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 mokėjimo priemonė, kuria atlikti ginčijami mokėjimai, buvo tik pareiškėjos žinioje. Dėl to, pačiai pareiškėjai neigiant ginčijamų mokėjimų autorizavimo aplinkybę, negalima daryti išvados, kad pareiškėjos mokėjimo priemone (kuri nustatytomis aplinkybėmis, ji galėjo būti pasisavinta ir (ar) ja neteisėtai pasinaudota) atlikti ginčijami mokėjimai buvo jos autorizuoti, t. y. inicijuoti ir patvirtinti pačios pareiškėjos sutikimu (kaip tai suprantama Mokėjimų įstatymo 29 straipsnio 1 dalies kontekste). Atsižvelgdamas į tai Lietuvos bankas daro išvadą, kad 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 (Mokėjimų įstatymo 37 straipsnio 3 dalis ir 39 straipsnio 3 dalis).

Aplinkybių ir duomenų, kaip ir šalių ginčo dėl to, kad pareiškėja galėjo veikti nesąžiningai arba tyčia, įskaitant sukčiavimą, nėra. Tai reiškia, kad, siekiant įvertinti, ar bankas pagrįstai atsisako kompensuoti pareiškėjos nuostolius, susijusius su 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.

Antrosios mokėjimo paslaugų direktyvos 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 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.[3]

Bankas savo sprendimą nekompensuoti pareiškėjos nuostolių grindžia aplinkybe, kad

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

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. Vertinamų aplinkybių kontekste pažymėtina, kad remiantis minėtų Mokėjimų įstatymo nuostatų analize, mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai tik tuo atveju, jei tenkinamos abi sąlygos, t. y. mokėtojas ne tik neįvykdo vienos ar kelių jam Mokėjimų įstatyme nustatytų pareigų, bet ir padaro tai elgdamasis nesąžiningai arba tyčia ar būdamas labai neatsargus. Taigi banko sprendimas nekompensuoti pareiškėjos nuostolių dėl neautorizuotų ginčijamų mokėjimų įvykdymo galėtų būti laikomas pagrįstu tik tuo atveju, jei būtų įrodyta, kad pareiškėja, tikėtina, atskleisdama tam tikrus personalizuotus savo mokėjimo priemonių saugumo duomenis ir taip sudarydama sąlygas tretiesiems asmenims panaudoti šiuos duomenis jos mokėjimo kortelei prie *Apple Pay* sistemos naujame mobiliajame įrenginyje pridėti, o vėliau ir inicijuoti ginčijamus mokėjimus, elgėsi itin aplaidžiai – buvo labai neatsargi.

Kaip minėta, 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.

Siekdamas tinkamai įvertinti ginčijamų mokėjimų įvykdymo aplinkybes Lietuvos bankas paprašė pareiškėjos papildomai paaiškinti, kokius veiksmus, galėjusius lemti ginčijamų mokėjimų įvykdymą, ji atliko iki jų inicijavimo (t. y. iki mokėjimo kortelės pridėjimo prie *Apple Pay* sistemos naujame įrenginyje), taip pat kokius savo mokėjimo priemonių personalizuotus saugumo duomenis galėjo atskleisti tretiesiems asmenims. Pareiškėja nurodė, kad niekada niekam nėra atskleidusi savo mokėjimo priemonių personalizuotų saugumo duomenų. 2022 m. kovo 4 d. iš banko SMS žinute ji negavo jokio vienkartinio saugos kodo, su prekybininku, kurio naudai įvykdyti ginčijami mokėjimai, niekada nebendravo ir nesiekė įsigyti iš jo paslaugų, todėl negalėjo jam atskleisti kokių nors savo mokėjimo priemonių personalizuotų saugumo duomenų. Ginčijami mokėjimai buvo inicijuoti ir įvykdyti dėl trečiųjų asmenų neteisėtų veiksmų.

Tačiau banko Lietuvos bankui pateikti vidaus sistemos duomenys patvirtina, kad pareiškėjos ginčijami mokėjimai inicijuoti naudojant *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, pagal banko pateiktus įrodymus, 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[4].

Tad nors pareiškėja teigė, kad jokių savo mokėjimo priemonių personalizuotų saugumo

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

duomenų niekam nėra atskleidusi, ginčijamų mokėjimų įvykdymo dieną iš banko jokio vienkartinio saugos kodo negavusi ir niekam jo nepateikusi, su prekybininku taip pat nebendravusi ir (ar) kokių nors savo duomenų jam neatskleidusi, 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 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 pažymėtina, kad, išanalizavus ginčo byloje esančius duomenis ir kitas ginčo nagrinėjimo metu nustatytas aplinkybes, pareiškėjos elgesys negali būti vertinamas kaip atsargus ir apdairus ar tik neatsargus. Kaip nustatyta, pridedant pareiškėjos mokėjimo kortelę prie *Apple Pay* sistemos naujame įrenginyje, buvo suvesti teisingi 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 mobilųjį 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). 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.

Dėl lėšų grąžinimo procedūros inicijavimo pagal Visa mokėjimo kortelių organizacijos taisykles

Papildomos galimybės mokėjimo kortelės turėtojui susigrąžinti mokėjimo kortele įvykdytų mokėjimo operacijų lėšas nustatytos tarptautinės mokėjimo kortelių organizacijos *Visa* taisyklėse. Vadovaudamasi šiomis taisyklėmis bankas, gavęs kliento prašymą, gali kreiptis į tarptautinę mokėjimo kortelių organizaciją *Visa* dėl lėšų grąžinimo procedūros taikymo[5]. Taigi banko veiksmus ginčijant mokėjimo kortele atliktas mokėjimo operacijas reglamentuoja minėtos *Visa* taisyklės ir nei Lietuvos Respublikos, nei Europos Sąjungos teisės aktai nereglamentuoja, kokiomis sąlygomis turi būti vykdomos tokios lėšų grąžinimo procedūros.

Pareiškėja, patarta banko klientų aptarnavimo specialistų, lėšų grąžinimo prašymą motyvavo tuo, kad neatpažįsta ginčijamų mokėjimų, t. y. jie įvykdyti neteisėtai. Bankas, pagrįsdamas sprendimą neinicijuoti lėšų grąžinimo procedūros pagal tarptautinės mokėjimo kortelių organizacijos *Visa* taisykles, nurodė, kad tokį sprendimą priėmė atsižvelgęs į tai, kad dėl mokėjimo kortelės pridėjimo prie *Apple Pay* sistemos ir pačių ginčijamų mokėjimų įvykdymo nebuvo nustatyta jokių apgaulingos veiklos pėdsakų, be to, banko vidaus sistemos duomenimis, ginčijami mokėjimai užregistruoti kaip autorizuoti. Bankas atkreipė dėmesį, kad, pagal tarptautinės mokėjimo kortelių organizacijos *Visa* paslaugų taisyklių vadovo (angl. *Visa Core Rules and Visa Product and Service Rules guide*) 11.7 skyrių, mokėjimo grąžinimo prašymas dėl sukčiavimo būdu pasisavintų lėšų negalioja, kai vartotojas dalyvauja mokėjimo operacijoje ir (ar) duoda leidimą atlikti (autorizuoja) mokėjimo operaciją. Nustatęs, kad pareiškėja patvirtino mokėjimo kortelės, kuria ir buvo atlikti ginčijami mokėjimai, pridėjimą prie *Apple Pay* sistemos pagal pareiškėjos ir banko sutartą saugesnio autentiškumo patvirtinimo procedūrą, bankas nusprendė, kad pareiškėjos prašymas nepatenka į tarptautinės mokėjimo kortelių organizacijos *Visa* ginčytinų mokėjimo operacijų kategoriją, todėl mokėjimų grąžinimo procedūra *Visa* nustatyta tvarka nebuvo inicijuota, o pareiškėjos prašymas atmestas.

Lietuvos banko vertinimu, ginčo byloje nėra duomenų, kurie leistų teigti, kad, bankui pabandžius inicijuoti lėšų grąžinimo procedūrą dėl pareiškėjos ginčijamų mokėjimų, tokia procedūra būtų buvusi sėkminga. Kitaip tariant, bankas atsiliepime pateikė motyvus – nurodė tarptautinės mokėjimo kortelių organizacijos *Visa* taisyklių nuostatas, pagal kurias ginčo procedūra šių taisyklių nustatyta tvarka dėl pareiškėjos ginčijamų mokėjimų nėra galima.

Įvertinus tai, kas išdėstyta, ir nustačius, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, darytina išvada, kad pareiškėjos reikalavimas bankui grąžinti ginčijamų mokėjimų sumą, t. y. 5050 Eur, yra nepagrįstas, todėl turi būti atmestas.

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

[5] Teisės aktai nereglamentuoja, kokiomis sąlygomis turi būti vykdomos tokios lėšų grąžinimo procedūros, nes tai nustato tam tikra mokėjimo kortelių organizacija savo parengtose lėšų grąžinimo (angl. *chargeback*) taisyklėse.