



**LIETUVOS BANKO
TEISĖS IR LICENCIJAVIMO DEPARTAMENTO
DIREKTORIUS**

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

2023 m. balandžio 19 d. Nr. 429-218
Vilnius

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

N u s t a t y t a:

2023 sausio 9 d. pareiškėjas per banko mobiliąją programėlę informavo banką, kad iš jo mokėjimo sąskaitos banke per pastarąsias kelias dienas buvo inicijuoti neautorizuoti mokėjimai. Banko specialistams paklausus, ar pareiškėjas gavo įtartinų žinučių ar nuorodų, pareiškėjas nurodė, kad negavo jokių nuorodų ir nespaudė jokios nuorodos, kuri jam būtų atrodžiusi įtartiną, tačiau taip pat paminėjo, kad anksčiau į savo mobilųjį įrenginį gavo žinutę su vienkartinio slaptažodžiu, skirtu mokėjimo kortelės pridėjimui prie *Google Pay* patvirtinti. Įvertinę, kad paskutiniai mokėjimai pareiškėjo sąskaitoje buvo atlikti per *Google Pay*, banko specialistai pareiškėjui paaiškino, kad mokėjimo kortelės pridėjimas prie *Google Pay* sistemos buvo galimas tik gavus vienkartinį kodą į pareiškėjo mobilųjį telefoną ir jį suvedus duomenų teisingumui ir atliekamam veiksmui patvirtinti.

Banko pateiktais duomenimis¹, netrukus pareiškėjas pakartotinai kreipėsi į banką per mobiliąją programėlę ir nurodė, kad jau pateikė bankui oficialų skundą dėl susidariusios situacijos, tačiau kartu prisipažino, jog vis dėlto pasidalino savo mokėjimo kortelės duomenimis bei SMS žinute gautu vienkartinio kodu po to, kai gavo žinutę į savo mobilųjį telefoną su nuoroda ir ją paspaudė. Vėliau pareiškėjas taip pat pateikė prašymą inicijuoti lėšų grąžinimo procedūrą (angl. *chargeback*).

Pareiškėjas ginčija 2023 m. sausio 6–9 d., panaudojant *Google Pay* atsiskaitymo metodą, mokėjimo kortele atliktų 19 mokėjimo operacijų, kurių bendra suma – 925 238 THB (12 831,83 GBP ir 11 396,64 Eur) (toliau – Ginčijami mokėjimai), nuskaičiuoti pervedimo mokesčiai sudaro 244,10 GBP ir 284,92 Eur. Atsižvelgiant į tai, kad trys iš šių Ginčijamų mokėjimų buvo atmesti (t. y. nenurašyti iš pareiškėjo mokėjimo kortelės sąskaitos), o paskutinis Ginčijamas mokėjimas grąžintas pardavėjo, faktiškai iš pareiškėjo mokėjimo kortelės sąskaitos nuskaičiuotų lėšų sumą sudaro 517 918 THB (12 807,19 GBP ir 28,90 Eur), be to, iš pareiškėjo mokėjimo kortelės sąskaitos nuskaičiuota ir 243,70 GBP bei 0,72 Eur pervedimo mokesčių.

2023 m. sausio 9 d. bankas priėmė sprendimą netenkinti pareiškėjo prašymų inicijuoti lėšų grąžinimo procedūrą, nes pareiškėjo Ginčijamų mokėjimų įvykdymo aplinkybės nepriskirtinos prie tarptautinės mokėjimo kortelių organizacijos „MasterCard“ taisyklėse nustatytų atvejų, kada tokia procedūra yra galima.

Pareiškėjas nesutinka su tokiu banko sprendimu ir atsisakymu kitaip kompensuoti pareiškėjo dėl Ginčijamų mokėjimų, kurių lėšos buvo nurašytos iš pareiškėjo mokėjimo kortelės sąskaitos ir negrąžintos, įvykdymo atsiradusius nuostolius. Pareiškėjas teigia buvęs apgautas sukčių siųstos SMS žinutės su nuoroda į suklastotą puslapį, kuriame pareiškėjas pripažįsta suvedęs savo mokėjimo kortelės duomenis ir atskleidęs vienkartinį SMS žinute gautą saugos kodą, tai įgalino trečiuosius asmenis pridėti jo mokėjimo kortelę prie *Google Pay* sistemos ir patvirtinti mokėjimus. Vis dėlto, pareiškėjo teigimu, jo mokėjimo kortelė prie *Google Pay* sistemos buvo pridėta be jo aktyvaus sutikimo ir žinios, o bankas nesustabdė sukčių kelias

¹ Pareiškėjo ir banko specialistų 2023 sausio 9 d. pokalbių banko mobiliojoje programėlėje kopija.

dienas jo mokėjimo kortele atliekamų Ginčijamų mokėjimų, todėl keipimesi pareiškėjas prašo, kad bankas atlygintų pareiškėjo nuostolius dėl įvykdytų Ginčijamų mokėjimų.

Bankas nesutinka tenkinti pareiškėjo reikalavimo. Bankas mano, kad pareiškėjo Ginčijami mokėjimai buvo jo tinkamai autorizuoti, todėl bankas negali būti įpareigotas gražinti pareiškėjui šių mokėjimų sumos. Kadangi veikė pagal teisės aktų bei paslaugų teikimo sąlygų nuostatas ir tinkamai įvykdė gautus mokėjimo nurodymus, t. y. nesant banko neteisėtų veiksmų, bankas teigia, kad negali būti keliamas ir banko civilinės atsakomybės klausimas, nes nėra tenkinama būtinoji civilinės atsakomybės taikymo sąlyga. Bankas papildomai pažymi, kad pareiškėjas, nepaisydamas SMS pranešime nurodytos informacijos dėl vienkartinio saugos kodo paskirties, taigi, veikdamas aplaidžiai ir nerūpestingai, pats savo aktyviais veiksmais trečiajam asmeniui suteikė galimybę pridėti jo mokėjimo priemonę prie *Google Pay* įrenginio.

Atsižvelgdamas į išdėstytą informaciją ir argumentus, bankas prašė atmesti pareiškėjo 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 42¹ straipsnyje reglamentuojamų patikrinimų, skirtų faktinėms aplinkybėms dėl Lietuvos banko prižiūrimo 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 gražinti pareiškėjui jo mokėjimo kortele, naudojant *Google Pay* mokėjimo metodą, atliktų Ginčijamų mokėjimų, kurių lėšos pareiškėjui nebuvo gražintos ir kurių bendra vertė sudaro 517 918 THB, sumą.

Pareiškėjas teigia nedavęs sutikimo atlikti Ginčijamus mokėjimus, neigia juos autorizavęs ir (ar) pridėjęs savo mokėjimo kortelę prie *Google Pay* sistemos iš naujo įrenginio. Pareiškėjas pripažįsta pagal SMS žinutėje pateiktą nuorodą atsidariusioje interneto svetainėje suvedęs savo mokėjimo kortelės duomenis bei atskira SMS žinute gautą vienkartinį saugos kodą, tačiau kartu mano, kad bankas nesiėmė pakankamai veiksmų tam, kad nesažiningi, be pareiškėjo žinios ir sutikimo atlikti Ginčijami mokėjimai nebūtų įvykdyti. Banko vertinimu, pareiškėjo Ginčijami mokėjimai laikytini autorizuotais, o bankas veikė pagal teisės aktų reikalavimus, todėl neturi pareigos kompensuoti pareiškėjo nuostolių.

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 pareiškėjo ir banko ginčą, Lietuvos banko vertinimu, būtina nustatyti, ar: 1) *Ginčijami mokėjimai laikytini autorizuotais*; 2) *bankas privalo gražinti pareiškėjui Ginčijamų mokėjimų sumą*; 3) *pagrįstai pareiškėjas teigia, kad banko paslaugos yra teikiamos nesaugiai ir tai galėjo nulemti pareiškėjo 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 pareiškėjo 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 kortelę terminalą (bekontaktis atsiskaitymas) ar atliekant kitus veiksmus su elektroniniu kortelių skaitytuvu. Šiuos veiksmus bankas laiko mokėtojo sutikimu atlikti mokėjimus iš banko sąskaitos². Atsižvelgiant į tai, kad bendroji sutartis (ją sudarančios banko privatiems klientams taikomos sąlygos) nustato banko ir pareiškėjo tarpusavio santykius, ir įvertinus tai, kad mokėjimo kortelės duomenys ir PIN kodo slaptažodis yra personalizuoti saugumo duomenys, kurie pripažįstami neskelbtiniais 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) pareiškėjo ir banko santykiuose laikytini pareiškėjo sutikimu įvykdyti mokėjimo operaciją tik tada, kai pats pareiškėjas pateikia mokėjimo kortelės duomenis ir (arba) suveda PIN kodo slaptažodį, norėdamas įvykdyti mokėjimo operaciją.

Banko kartu su atsiliepimu pateiktais vidaus sistemos duomenimis, visi pareiškėjo Ginčijami mokėjimai atlikti tuo pačiu mobiliuoju įrenginiu (įrenginio pavadinimas matomas banko sistemoje „|samsung|samsung|SM-A236E“), kuris kaip *Google Pay* mokėjimo įrenginys prie *Google Pay* sistemos buvo pridėtas ir autorizuotas, kaip nurodė bankas, paties pareiškėjo dieną prieš įvykdant pirmąjį Ginčijamą mokėjimą, t. y. 2023 m. sausio 5 d.

Pareiškėjas neigia autorizavęs Ginčijamus mokėjimus ar pridėjęs (siekęs pridėti) savo mokėjimo kortelę prie *Google Pay* sistemos, tačiau pripažįsta prieš Ginčijamų mokėjimų įvykdymą tretiesiems asmenims atskleidęs (pagal nuorodą SMS žinutėje atsidariusioje suklastotoje pašto siuntų bendrovės interneto svetainėje suvedęs) savo mokėjimo kortelės duomenis, o vėliau ir atskira SMS žinute gautą saugos kodą.

Kaip paaiškino bankas atsiliepime, norėdamas pridėti mokėjimo kortelę prie *Google Pay*, asmuo turi atlikti aktyvius veiksmus, numatytus *Google Pay* sąlygose³: 1) įrenginyje, kuriuo siekiama atlikti *Google Pay* mokėjimą, reikia įvesti mokėjimo kortelės duomenis. Tai galima atlikti, kortelės duomenis, t. y. kortelės numerį, saugos kodą CVV, kita, suvedant rankiniu būdu arba nuskaitant (nufotografuojant) mokėjimo kortelę; 2) suvedęs mokėjimo kortelės duomenis, asmuo turi perskaityti mokėjimo sąlygas (angl. Issuer Terms) ir su jomis sutikti; 3) kad būtų patvirtinti mokėjimo kortelės duomenys ir mokėjimo metodas, bankas patikrina pateiktą informaciją. Nustačius, kad pateikta mokėjimo kortelė yra aktyvi ir duomenys teisingi, asmuo turi atlikti banko, kuris išdavė mokėjimo kortelę, nurodymus. Šiuo atveju – įvesti vienkartinį saugos kodą (kuris galioja 30 min. po kodo išsiuntimo), kuris yra išsiunčiamas į telefono numerį, susietą su mokėjimo kortelės savininko banko sąskaita. Tiek banko, tiek paties pareiškėjo pateiktais duomenis, pareiškėjui jo bankui nurodytu telefonu numeriu buvo išsiųsta SMS žinutė su vienkartinio saugos kodu, tai, banko teigimu, reiškia, kad pirmiau nurodyti veiksmai pareiškėjo mokėjimo kortelei prie *Google Pay* įrenginio pridėti – pareiškėjo mokėjimo kortelės duomenų (numeris, CVV kodas) suvedimas, taip pat buvo atlikti. Tinkamai atlikus mintus veiksmus, gaunamas pranešimas, kad mokėjimo kortelė pridėta ir ja galima sėkmingai naudotis.

Atsiliepime, net ir atsižvelgdamas į tai, kad visi Ginčijami mokėjimai buvo inicijuoti prie *Google Pay* sistemos pridėjus pareiškėjo mokėjimo kortelę naujame įrenginyje, kuris, kaip nurodo bankas, nepriklauso pareiškėjui, bankas teigė, kad šie mokėjimai laikytini autoriztais, nes mokėjimo kortelė inicijuojant Ginčijamus mokėjimus buvo pareiškėjo žinioje, o prie *Google Pay* sistemos pridėta, suvedus vienkartinį saugos kodą, atsiųstą SMS žinute į pareiškėjo mobilųjį telefoną.

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

Kaip nurodo pareiškėjas, prieš pridėdamas jo mokėjimo kortelę prie *Google Pay* sistemos naujame įrenginyje ir atitinkamai prieš įvykdant Ginčijamus mokėjimus, pareiškėjas SMS žinute

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. 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 <...>“

³ https://support.google.com/googlepay/answer/9039712?visit_id=638168132866517827-1780936203&rd=1

gavo tariamą pašto siuntų bendrovės pranešimą, kad turi susimokėti 1,20 Eur už prekę, kuri turi būti pristatyta pareiškėjui. Sekdamas būtent minėtoje SMS žinutėje pateiktus nurodymus ir paspaudęs joje pateiktą nuorodą, pareiškėjas atsidariusioje interneto svetainėje suvedė savo mokėjimo kortelės duomenis ir vėliau SMS žinute gautą vienkartinį saugos kodą. Tiek bankui kartu su pretenzija, tiek ir Lietuvos bankui kartu su kreipimusi pareiškėjas pateikė pirmiau minėtos trečiųjų asmenų, apsimesusių pašto siuntų bendrove, siųstos SMS žinutės ir pagal joje pateiktą nuorodą atsidariusios interneto svetainės ekrano vaizdus.

Taigi, nors, ginčo bylos duomenimis, pareiškėjo mokėjimo kortelė prie *Google Pay* sistemos naujame įrenginyje galėjo būti pridėta suvedant ne tik šios kortelės duomenis (kortelės numerį, CVC kodą), bet ir banko į pareiškėjo mobilųjį telefoną SMS žinute atsiųstą vienkartinį saugos kodą, to neginčija ir pats pareiškėjas, nustatyti ir banko neginčijami duomenys leidžia pagrįstai abejoti, ar mokėjimo priemonė, kuria atlikti Ginčijami mokėjimai, buvo tik pareiškėjo žinioje. Dėl to, pačiam pareiškėjui neigiant Ginčijamų mokėjimų autorizavimo aplinkybę ir esant pagrįstų duomenų apie įvykusį sukčiavimo atvejį, taigi, kad pareiškėjo mokėjimo priemone ir jos personalizuotais saugumo duomenimis, be pareiškėjo žinios ir nesant jo valios, galėjo neteisėtai pasinaudoti tretieji asmenys, ir negalima daryti išvados, kad pareiškėjo mokėjimo kortele atlikti Ginčijami mokėjimai buvo jo autorizuoti, t. y. inicijuoti ir patvirtinti esant paties pareiškėjo 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 pareiškėjo teisės į Ginčijamų mokėjimų sumos gražinimą

Pagal Mokėjimų įstatymo 38 straipsnio 1 dalį, joje nurodytomis sąlygomis ir tvarka, mokėtojo mokėjimo paslaugų teikėjas privalo gražinti 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 nesažiningai arba tyčia ar dėl didelio neatsargumo neįvykdęs vienos ar kelių šio įstatymo 34⁴ straipsnyje nustatytų pareigų, susijusių su mokėjimo priemonės naudojimu.

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 nesažiningai 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 gražinti 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 neįvykdė vienos ar kelių jam Mokėjimų įstatyme nustatytų pareigų, bet ir padaro tai elgdamasis nesažiningai 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 pareiškėjas galėjo veikti nesažiningai arba tyčia, įskaitant sukčiavimą, nėra. Bankas sprendimą nekompensuoti pareiškėjo nuostolių grindžia vertinimu, kad Ginčijami mokėjimai buvo autorizuoti tinkamai. Be to, bankas mano, kad pareiškėjo elgesiui būdingas ir didelis neatsargumas.

Tai reiškia, kad, atsižvelgiant į pirmiau minėtas Mokėjimų įstatymo nuostatas, siekiant įvertinti, ar bankas pagrįstai atsisako kompensuoti pareiškėjo nuostolius, susijusius su

⁴ 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).

Ginčijamų mokėjimų įvykdymu, ir ar pareiškėjui galėtų būti taikoma Mokėjimų įstatymo 39 straipsnio 3 dalis, būtina nustatyti, ar pareiškėjo 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 jo reikalaujami atlyginti nuostoliai turėtų tekti pačiam pareiškėjui.

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 – pareiškėjas. Atsižvelgiant į tai, manytina, kad pareiškėjo elgesys būtų laikomas atitinkančiu mokėjimo priemonės išdavimą ir naudojimą reglamentuojančio susitarimo sąlygas, jei būtų nustatyta, kad jis 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.

Pareiškėjas, pateikdamas paaiškinimus dėl Ginčijamų mokėjimų įvykdymo aplinkybių ir kartu dėl bankui keliamo reikalavimo pagrįstumo, nurodė, kad 2023 m. sausio 5 d., t. y. dieną prieš pridėdamas jo mokėjimo kortelę prie *Google Pay* ir įvykdant pirmąjį Ginčijamą mokėjimą, jis SMS žinute gavo tariamai pašto siuntų bendrovės siųstą pranešimą, kad pareiškėjas turi sumokėti 1,20 Eur už prekę, kuri jam turi būti netrukus pristatyta. Pareiškėjo teigimu, kadangi jis buvo neseniai užsakęs prekių internetu, gautas pranešimas jam nepasirodė įtartinas, todėl jis paspaudė gautoje SMS žinutėje pateiktą nuorodą ir pagal ją atsidariusioje suklastotoje pašto siuntų bendrovės interneto svetainėje suvedė savo mokėjimo kortelės duomenis, o vėliau ir SMS žinute gautą vienkartinį saugos kodą. Atsižvelgiant į tai, galima daryti išvadą, kad Ginčijami mokėjimai, pareiškėjo vertinimu, buvo inicijuoti ir įvykdyti dėl trečiųjų asmenų neteisėtų veiksmų, tretiesiems asmenims galimai neteisėtai nusavinus jo mokėjimo priemonių personalizuotus saugumo duomenis.

Vis dėlto, išanalizavęs ginčo byloje esančius duomenis ir kitas nustatytas aplinkybes, net ir įvertinęs tai, kad trečiųjų asmenų (sukčių) veiksmai, atsiunčiant SMS žinutę su nuoroda į suklastotą pašto siuntų bendrovės interneto puslapį tariamam atsikaitymui už internetu užsakytos prekės pristatymą, iš tiesų galėjo sukurti klaidinančią pirminę įspūdį kaip teisėti, Lietuvos bankas mano, kad pareiškėjo elgesys negali būti vertinamas kaip atsargus ir apdairus ar tik neatsargus. Nustatyta, kad, pridėdamas pareiškėjo mokėjimo kortelę prie *Google 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 pareiškėjo telefono numeriu. Ginčo bylos duomenimis, kartu su vienkartinio saugos kodu pareiškėjui SMS žinutėje buvo nurodyta šio kodo paskirtis ir perspėjimas jo neperduoti tretiesiems asmenims: „Šis kodas bus naudojamas jūsų kortelei pridėti prie kito *Google Pay* įrenginio. Nesidalinkite šiuo kodu su niekuo, net jei jie teigia esantys iš *Revolut*. Niekur jo neįveskite, nebent norite pridėti savo kortelę prie naujo įrenginio. *Revolut* patvirtinimo kodas, skirtas *Google Pay*: xxxxxx.“⁵

Pareiškėjas pažymi, kad vienkartinį saugos kodą, gautą SMS žinute, jo telefonas automatiškai nukopijavo į tokių duomenų prašančią interneto puslapį (galimai suklastotą pašto siuntų bendrovės interneto puslapį), tad savo aktyvaus sutikimo pridėti mokėjimo kortelę prie *Google Pay* sistemos pareiškėjas teigia nedavęs. Vis dėlto ginčo byloje nėra duomenų, kurie leistų tokius pareiškėjo teiginius patvirtinti. Kita vertus, SMS žinutėje, kurioje pareiškėjui buvo nurodytas vienkartinis saugos kodas, buvo ne tik aiškiai nurodyta, kokiam tikslui yra siunčiamas šis kodas, t. y. pareiškėjo mokėjimo kortelei prie *Google Pay* įrenginio pridėti, bet ir pateiktas įspėjimas šio kodo niekam neatskleisti ir niekur nesuvesti, jei neketinama atlikti aprašyto

⁵ Tekstas anglų k.: „This code will be used to add your card to another *Google Pay* device. Don't share this code with anyone, even if they claim to be from *Revolut*. Don't enter anywhere unless you want to add your card to a new device. *Revolut* verification code for *Google Pay*: xxxxxx.“

veiksmo (t. y. pridėti mokėjimo kortelės prie *Google Pay* įrenginio). Informacijos, kokiam tikslui skirtas pareiškėjui SMS žinute atsiųstas vienkartinis saugos kodas, pareiškėjas galėjo nematyti tik dėl to, kad buvo itin neatidus ir, neperskaitęs žinutės teksto ar jį ignoravęs (jo nepaisęs), besąlygiškai pasitikėjo pagal SMS žinutėje atsidariusio interneto puslapio ir jame pateiktų nurodymų atskleisti savo mokėjimo priemonių konfidencialius duomenis patikimumu. Pareiškėjas teigia laukęs internetu užsakytos prekės pristatymo, todėl neabejojęs tariamai pašto siuntų bendrovės vardu atsiųstos SMS žinutės su nuoroda patikimumu. Vis dėlto duomenų, kad šioje SMS žinutėje būtų nurodyta būtent pareiškėjo užsakyta prekė, ir priežasčių, kodėl pareiškėjas būtų turėjęs papildomai sumokėti už jos pristatymą, ir juo labiau, kodėl už papildomą atsiskaitymą už prekės pristatymą jis būtų turėjęs ne tik nurodyti savo mokėjimo kortelės duomenis, bet ir vienkartinį SMS žinute gautą saugos kodą, skirtą mokėjimo kortelės pridėjimui prie *Google Pay* sistemos patvirtinti, ginčo byloje nėra, paaiškinimų nepateikė ir pats pareiškėjas.

Pareiškėjas teigia, nesuabejojęs gauta SMS žinute ir nepatikrinęs pagal nuorodą joje atsidariusio interneto puslapio ir jame pateiktų nurodymų patikimumo, atskleidęs pirmiau minėtus konfidencialius duomenis ir šie veiksmai įgalino trečiuosius asmenis tiek susieti pareiškėjo mokėjimo kortelę su *Google Pay* mokėjimo metodu, tiek ir vėliau įvykdyti Ginčijamus mokėjimus. Svarbu ir tai, kad pareiškėjas SMS žinute gavo vienkartinį saugos kodą jo mokėjimo kortelės pridėjimui prie *Google Pay* įrenginio patvirtinti, nors, kaip kreipimesi nurodo, pats naudojasi *Apple iPhone* telefonu, tačiau tokia aplinkybė taip pat nesukėlė jokių įtarimų pareiškėjui⁶. Be to, kaip atskleidžia pareiškėjas, SMS žinutę su vienkartinio saugos kodu jo mokėjimo kortelei prie *Google Pay* įrenginio pridėti jis gavo dieną prieš įvykdant pirmąjį Ginčijamą mokėjimą, tad jei nebūtų elgęsis itin neapdairiai, būtų turėjęs galimybę pastebėti, kad nepagrįstai pasitikėdamas gautais nurodymais galėjo atskleisti tretiesiems asmenims savo mokėjimo priemonių konfidencialius duomenis ir taip išvengti Ginčijamų mokėjimų įvykdymo, tačiau to nepastebėjo.

Vadinasi, tretieji asmenys be pareiškėjo žinios galėjo neteisėtai pasinaudoti pareiškėjo mokėjimo kortele ir įvykdyti Ginčijamus mokėjimus tik dėl to, kad pareiškėjas, būdamas labai neatsargus, netinkamai vykdė Mokėjimų įstatyme (34 straipsnis) ir banko privatiems klientams taikomose sąlygose įtvirtintus mokėjimo kortelės saugaus naudojimo reikalavimus. Taigi, pareiškėjas, elgdamasis labai neatsargiai, neišsaugojo jo vardu išduotos mokėjimo kortelės duomenų konfidencialumo, t. y. nesiėmė tų saugumo priemonių, kurių privalėjo imtis, kad būtų tinkamai apsaugoti jam suteiktos mokėjimo kortelės duomenys, ir tretiesiems asmenims suteikė (nurodė) vienkartinį saugos kodą, kurį gavo į jam priklausančią telefono numerį trumpąja SMS žinute, nors ta pačia SMS žinute buvo papildomai įspėtas apie būtinybę saugoti ir niekam neatskleisti atsiųsto saugos kodo.

Konstatavus, kad pareiškėjas, nesilaikydamas jam, kaip mokėtoju, 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) pareiškėjui neautorizuotų Ginčijamų mokėjimų lėšų ir pareiškėjo reikalavimas, kad bankas kompensuotų pareiškėjui iš mokėjimo kortelės sąskaitos nurašytų ir negrąžintų Ginčijamų mokėjimų lėšas – 517 918 THB, atmestinas kaip nepagrįstas.

3. Dėl banko teikiamų paslaugų saugumo

Pagrįsdamas bankui keliamą reikalavimą, pareiškėjas kreipimesi taip pat teigia, kad bankas nesiėmė pakankamai priemonių tam, kad apsaugotų jo banko sąskaitoje esančias lėšas, nesustabdė nė vieno iš per kelias dienas atliktų Ginčijamų mokėjimų.

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 kuo geriau apsaugoti nuo neautorizuotų ir (ar) nesąžiningų mokėjimo operacijų ir turėtų visas galimybes ginčijamų

⁶ *Google Pay* atsiskaitymo metodas suderinamas su *Android* įrenginiais, o *Apple iPhone* įrenginiai – su *Apple Pay* atsiskaitymo metodu.

mokėjimo operacijų lėšas bandyti susigražinti, ypač sukčiavimų elektroninėje erdvėje atvejais⁷.

Paaikškinimuose dėl teikiamų mokėjimo paslaugų saugumo ir klientų atliekamų mokėjimo operacijų stebėsenos bankas nurodė, kad mokėjimo operacijos kortele yra stebimos gyvai banko automatizuotos saugumo sistemos, kuri, veikdama autonomiškai pagal tam tikras nustatytas „taisykles“ (kompiuterinius algoritmus), atlieka potencialios sukčiavimo rizikos vertinimą kiekvienos mokėjimo operacijos kortele atžvilgiu. Identifikavusi įtartinos kilmės mokėjimo operacijas kortele, toliau automatizuota saugumo sistema imasi šių veiksmų: mokėjimo operacijos atšaukimo, vėliau – mokėjimo kortelės užblokavimo ir kliento informavimo per banko mobiliąją programėlę bei elektroniniu paštu apie atšauktą mokėjimo operaciją ir užblokuotą mokėjimo kortelę.

Bankas paaiškino, kad banko įdiegta automatizuota saugumo sistema, prieš priimdama sprendimą vertinti mokėjimo operaciją kaip įtartiną, atsižvelgia į mokėjimo operacijos savybes (pavyzdžiui, naudos gavėjo informacija, suma, paros laikas); kliento ypatybes, t. y. palygina konkrečios mokėjimo operacijos reikšmę (ekonominė paskirtis) su mokėjimo operacijų istorija; naudos gavėjo ir prekybininko kategoriją, t. y. palygina inicijuojamą mokėjimo operaciją su visomis praeityje inicijuotomis įtartinomis ir neįtartinomis mokėjimo operacijomis nurodytam naudos gavėjui arba prekybininkui.

Šiuo atveju, kaip teigia bankas, analizuojant pareiškėjo mokėjimo operacijų istoriją, matyti, kad didžioji dalis pareiškėjo mokėjimo operacijų yra skirtos kasdienėms išlaidoms bei asmeninio pobūdžio pirkiniams. Bankas pažymi, kad Ginčijami mokėjimai pagal sumą, palyginti su pareiškėjo praeityje inicijuotomis mokėjimo operacijomis, niekuo neišsiskyrė.

Kaip minėta, nagrinėdamas ginčus Lietuvos bankas 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 pareiškėjo nurodytą aplinkybę, kad bankas nesiėmė reikiamų veiksmų, kad apsaugotų pareiškėjo banko sąskaitose esančias lėšas, o įvykdydamas Ginčijamus mokėjimus bankas būtų pažeidęs finansų rinką reglamentuojančių teisės aktų reikalavimus. Be to, kaip nurodė bankas, jokių techninių trikdžių atliekant Ginčijamus mokėjimus nebuvo užfiksuota, banko vidaus sistemose taip pat nebuvo užfiksuota jokių trečiųjų asmenų įsilaužimo į pareiškėjo mokėjimo kortelės sąskaitą banko programėlėje požymių.

Verta atkreipti dėmesį ir į tai, kad faktas, jog, vykdydamas trečiųjų asmenų apgaulingus nurodymus, pareiškėjas sudarė sąlygas savo mokėjimo kortelę pridėti prie *Google Pay* įrenginio ir įvykdyti visus 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 ir mokėjimo kortelės užblokavimo apie tai pačiam pareiškėjui informavus banką. Duomenų, kaip konstatuota pirmiau, kad banko paslaugos vykdančios Ginčijamus mokėjimus buvo teikiamos nesaugiai (banko saugumo sistemos neveikė), nenustatyta.

Remdamasis tuo, kas išdėstyta, ir vadovaudamasis Lietuvos Respublikos vartotojų teisių apsaugos įstatymo 27 straipsnio 1 dalies 3 punktu, Lietuvos banko valdybos 2012 m. sausio 26 d. nutarimo Nr. 03-23 „Dėl Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių patvirtinimo“ 2 punktu ir šiuo nutarimu patvirtintų Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių 59.3 papunkčiu, n u s p r e n d ž i u:

Atmesti pareiškėjo X. X. 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

⁷ 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.

bendrosios kompetencijos teismui prašydama nagrinėti tapatų ginčą iš esmės.

Direktorius

Arūnas Raišutis