LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

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

2023-01-26 Nr. 429-54
Vilnius

Lietuvos bankas gavo X. X. (toliau – pareiškėja) 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. rugsėjo 8 d. iš pareiškėjos atsiskaitomosios sąskaitos, esančios banke, buvo atlikta trylika mokėjimo operacijų (bendra suma – 57 507,03 GBP) į kituose bankuose atidarytas atsiskaitomąsias sąskaitas skirtingiems naudos gavėjams (toliau – mokėjimo operacijos).

Tą pačią dieną pareiškėja kreipėsi į banką ir nurodė, kad galimai tapo sukčių auka. Pareiškėja teigė, kad su ja susisiekė asmenys, prisistatę banko darbuotojais, ir prašė pervesti lėšas į naują, saugią pačios pareiškėjos sąskaitą. Pareiškėja teigė beveik valandą kalbėjusi telefonu su tariamu banko darbuotoju, jis padėjo atsidaryti antrąją sąskaitą banke, o vėliau ir atlikti mokėjimo operacijas. Pareiškėja teigė visus duomenis gavusi į banko žinučių srautą ir nurodė, kad tretiesiems asmenims neatskleidė jokių duomenų ir jokios asmeninio pobūdžio informacijos, susijusios su asmenine mokėjimo sąskaita.

Gavęs pareiškėjos kreipimąsi, bankas pradėjo vidinį tyrimą dėl galimo sukčiavimo. Įvertinęs pareiškėjos pateiktus duomenis, bankas jos pasiteiravo, ar lėšos pasiekė sąskaitą kitame banke. Tačiau pareiškėja pateikė duomenis, patvirtinančius, kad tretieji asmenys jai nurodė, kad lėšos neva turėjo nukeliaut į jos antrąją asmeninę sąskaita banke, o ne į kitas sąskaitas. Įvertinęs šias aplinkybes, bankas patikrino turimus duomenis ir nustatė, kad pareiškėjos vardu nebuvo atidarytos kitos sąskaitos banke, ir apie tai informavo pareiškėją.

Bankas papildomai paprašė pateikti duomenis apie visus įrenginius, kuriais pareiškėja, jungdamasi prie banko paskyros, naudojosi ir naudojasi šiuo metu. Taip pat bankas prašė pateikti duomenis, ar pareiškėja dalijosi asmeninio pobūdžio informacija per įtartinus šalinius, pavyzdžiui, trumpąsias SMS žinutes, elektroninius laiškus ir pan.

Pareiškėja bankui nurodė jos įrenginius ir teigė niekam neatskleidusi asmeninio pobūdžio informacijos.

Bankas pakartotinai pasiteiravo pareiškėjos, ar ji savo telefone įdiegė kokią nors trečiųjų asmenų pasiūlytą programinę įrangą, pvz., „Quick Viewer Team Support", ir ar atskleidė kokią kitą informaciją, tačiau pareiškėja tai paneigė. Pareiškėja akcentavo tik savo įrenginyje patvirtindavusi mokėjimo operacijas, kai atsirasdavo iššokantys pranešimai. Pareiškėjai buvo pasiūlyta dėl galimo sukčiavimo atvejo kreiptis ir į teisėsaugos institucijas.

2022 m. rugsėjo 16 d., atlikęs vidinį tyrimą, bankas priėmė sprendimą negrąžinti mokėjimo operacijų metu pareiškėjos prarastų lėšų. Bankas tokį sprendimą priėmė remdamasis tuo, kad pareiškėja, atlikdama mokėjimo operacijas, pati jas autorizavo ir buvo tinkamai informuota, kad mokėjimo operacijos yra įtartinos ir pareiškėja gali tapti sukčiavimo auka bei prarasti savo siunčiamas lėšas. Bankas taip pat informavo pareiškėją, kad susisiekė su naudos gavėjų bankais ir dėjo visas pastangas, kad atgautų pareiškėjos prarastas lėšas, tačiau lėšų

[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*.

atgauti nepavyko.

Po priimto sprendimo pareiškėja 2022 m. spalio 15 d. pakartotinai kreipėsi į banką ir prašė sprendimą apsvarstyti pakartotinai, tačiau bankas 2022 m. spalio 28 d. pareiškėjai pateikė atsakymą, kad priimtas sprendimas yra pagrįstas ir keičiamas nebus. Pareiškėja su tuo nesutiko, todėl tarp šalių kilo ginčas.

Kreipimesi į Lietuvos banką pareiškėja prašo rekomenduoti bankui grąžinti atliekant mokėjimo operacijas pareiškėjos prarastas lėšas. Pareiškėja kreipimesi iš esmės pakartojo bankui nurodytas aplinkybes. Pareiškėjos nuomone, bankas privalo prisiimti atsakomybę už tai, kad neužtikrino pareiškėjos atsiskaitomosios sąskaitos saugumo ir tretieji asmenys galėjo atlikti mokėjimo operacijas.

Atsiliepime į pareiškėjos kreipimąsi bankas nurodo nesutinkąs su pareiškėjos reikalavimu ir prašo jį atmesti. Banko teigimu, pareiškėja net kelis kartus buvo tinkamai informuota apie abejotiną bei įtartiną mokėjimo operacijų pobūdį ir kad atlikus minėtus mokėjimus egzistuoja reali tikimybė, jog pareiškėja taps sukčių auka ir praras pervestas lėšas.

Banko vidinių sistemų duomenimis, pareiškėjai atliekant pirmąsias mokėjimo operacijas naujiems gavėjams, banko automatizuota APP (angl. *Authorised push payment*) saugumo sistema (toliau – APP sausumo sistema) buvo sėkmingai aktyvuota. Banko turimais duomenimis, pareiškėja patvirtino, kad pasitiki kiekvienu naudos gavėju. Taip pat bankas nurodė, kad visų mokėjimo operacijų metu nurodyti gavėjo duomenys neatitiko realių naudos gavėjo duomenų, todėl atitinkamai pareiškėjai buvo parodyti pranešimai apie mokėjimo gavėjo vardo nesutapimą (angl. *confirmation of payee*)[2]. Banko teigimu, pareiškėja patvirtino naujus naudos gavėjus po šių pranešimų.

Taip pat bankas nurodo, kad, pirmą kartą atliekant mokėjimo operacijas naujiems naudos gavėjams, įsijungė ir papildomas APP saugumo sistemos veiksnys, kuris įspėjo apie galimai pareiškėjos atžvilgiu vykdomą sukčiavimo ataką. Remiantis pareiškėjai išsiųstais APP saugumo sistemos pranešimais, pareiškėja turėjo pasirinkti mokėjimo operacijos paskirtį, t. y. pasirinkti iš 6 pasiūlytų variantų: „1) *Transfer to a „Safe account*"; 2) *Payment for Goods and Services*; 3) *Investment*; 4) *Paying MHRC or Tax authority*; 5) *Paying the Police or Law enforcement*; 6) *Something Else*". Banko teigimu, pareiškėja 5 kartus pasirinko „Prekės ir paslaugos" ir vieną kartą „Investavimas" mokėjimo operacijų paskirtį.

Atitinkamai bankas papildomai išsiuntė pranešimus, kad pareiškėja turi būti itin budri, ir pateikė tolimesnius galimus variantus: 1) susipažinti su visuotinai paplitusių bei vykdomų sukčiavimo aferų aprašymais banko interneto tinklalapyje; 2) pasikonsultuoti dėl atliekamo mokėjimo su banko klientų aptarnavimo specialistais; 3) nutraukti inicijuoto mokėjimo vykdymą; 4) nepriklausomai nuo visų įspėjimų bei pareiškėjai suprantant ir sąmoningai prisiimant riziką bei su ja susijusius galimus neigiamus padarinius, patvirtinti ir inicijuoti vykdyti mokėjimą. Bankas nurodo, kad pareiškėja, suprasdama ir sąmoningai prisiimdama riziką bei su ja susijusius galimus neigiamus padarinius, pasirinko patvirtinti mokėjimo operacijas.

Taip pat bankas pažymi ir tai, kad mokėjimo operacijos buvo inicijuotos naudojantis interneto naršykle, o ne įprastu pareiškėjos įrenginiu, todėl šiuo atveju buvo taikomas papildomas autorizacijos patvirtinimas. Banko teigimu, pareiškėja, norėdama autorizuoti mokėjimą, turėjo įvesti vienkartinį slaptažodį (kodą), kuris yra išsiunčiamas trumpąja SMS žinute į asmeninį telefono numerį, kurį klientas pateikia bankui atidarant mokėjimo sąskaitą. Vienkartiniai slaptažodžiai yra individualiai sugeneruojami pagal atliekamą veiksmą ir galioja tam tikrą laiko tarpą. Bankas pažymėjo, kad, pagal jų turimą informaciją, pareiškėjai buvo išsiųsta 12 vienkartinių slaptažodžių. Banko teigimu, pati pareiškėja autorizacijos klausimo neginčijo, priešingai, nurodė, kad tariamas banko atstovas inicijuodavo mokėjimo operacijas, o pareiškėja, gavusi atitinkamus iššokančius pranešimus, juos autorizuodavo. Taigi, bankas mano, kad pati pareiškėja nepaisė jai atsiųstų APP saugumo sistemos pranešimų ir savo veiksmais patvirtino mokėjimo operacijas.

Bankas papildomai pateikė duomenis, kad pareiškėja buvo labai neatsargi. Banko teigimu, trečiojo asmens galimybė prisijungti prie pareiškėjos asmeninės mokėjimo sąskaitos be pareiškėjos aktyvių veiksmų nebūtų buvusi įmanoma, nes bankas į pareiškėjos mobilųjį telefoną išsiuntė net 3 įspėjimus ir prašymą patvirtinti, kad būtent ji jungiasi prie pareiškėjos asmeninės sąskaitos per banko programėlės naršyklės versiją, todėl pareiškėja turėjo galimybę suvokti, kokius veiksmus atlieka. Taigi, banko teigimu, dėl nurodytų priežasčių pareiškėja buvo labai

[2] Pranešimo tekstas: *„Sąskaitos pavadinimas nesutampa. Gavėjo bankas nurodė, kad jūsų įvestas vardas nesutampa su sąskaitos pavadinimu. Dar kartą patikrinkite išsamią informaciją it tęskite tik tuo atveju, jei esate tikri, kad gavėjas yra patikimas*".

neatsargi, todėl bankui nekyla pareiga grąžinti tinkamai įvykdytų mokėjimo operacijų metu pervestų lėšų.

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

Vadovaujantis Lietuvos banko valdybos 2012 m. sausio 26 d. nutarimu Nr. 03-23 patvirtintų Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių 45 punktu, vartojimo ginčai Lietuvos banke nagrinėjami laikantis rungimosi, ginčų nagrinėjimo operatyvumo, koncentracijos, ekonomiškumo ir bendradarbiavimo principų. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Kaip matyti iš Lietuvos bankui pateiktų dokumentų ir informacijos, šalių ginčas kilo dėl banko atsisakymo pareiškėjai grąžinti iš banko sąskaitos pareiškėjos inicijuotų ir banko įvykdytų mokėjimo operacijų metu prarastas lėšas.

Pareiškėja neigia autorizavusi mokėjimo operacijas bei tvirtina, kad lėšos iš jos atsiskaitomosios sąskaitos buvo nurašytos dėl to, kad tretieji asmenys turėjo galimybę prisijungti prie pareiškėjos mokėjimo sąskaitos ir taip inicijuoti bei patvirtinti mokėjimo operacijas. Dėl šios priežasties pareiškėja prašo banko grąžinti mokėjimo operacijų metu tretiesiems asmenims pervestas lėšas. Atsiliepime bankas nurodo, kad mokėjimo operacijos įvykdytos ne dėl sutrikimų banko sistemoje ar saugumo spragų jose, o dėl pareiškėjos veiksmų, kuriais tretiesiems asmenims pareiškėjos aktyviais veiksmais buvo leista prisijungti prie jos atsiskaitomosios sąskaitos ir pareiškėja atskleidė vienkartinius saugos kodus, kuriais buvo patvirtintos mokėjimo operacijos, dėl to tretieji asmenys įgijo galimybę savo įrenginiu inicijuoti ir patvirtinti mokėjimo operacijas pareiškėjos sąskaitoje.

Mokėjimo paslaugų teikėjų veiklą ir atsakomybę, mokėjimo paslaugas, jų teikimo sąlygas ir informavimo apie šias sąlygas reikalavimus, mokėjimo operacijų autorizavimą ir vykdymą, mokėjimo paslaugų vartotojų ir mokėjimo paslaugų teikėjų teises ir pareigas, susijusias su mokėjimo paslaugomis, kai mokėjimo paslaugų teikimas yra verslas, reglamentuoja Lietuvos Respublikos mokėjimų įstatymas.

Mokėjimų įstatymo 29 straipsnio 1 dalyje nustatyta, kad mokėjimo operacija laikoma autorizuota tik tada, kai mokėtojas duoda sutikimą įvykdyti mokėjimo operaciją. Jeigu mokėtojo sutikimo įvykdyti mokėjimo operaciją nėra, laikoma, kad mokėjimo operacija yra neautorizuota (Mokėjimų įstatymo 29 straipsnio 2 dalis).

Bankas atsiliepime nurodo, kad pareiškėjos mokėjimo operacijos buvo inicijuotos naudojantis banko programėlės naršyklės versija, kuria, kaip teigia pareiškėja, ji nesinaudoja. Šių aplinkybių neginčija nei bankas, nei pareiškėja. Taigi, šalių neginčijamomis aplinkybėmis, mokėjimo operacijos buvo inicijuotos ir patvirtintos trečiųjų asmenų, jiems neteisėtu būdu per banko programėlės naršyklės versiją prisijungus prie pareiškėjos banko sąskaitos. Akivaizdu, kad mokėjimo operacijų inicijavimas ir patvirtinimas neatitiko pačios pareiškėjos valios, nors formaliai (pagal išorinius požymius) ir sutapo su pareiškėjos ir banko sutarta sutikimo atlikti mokėjimo operacijas davimo forma ir tvarka.

Dėl šios priežasties Lietuvos bankas daro išvadą, kad mokėjimo operacijos buvo atliktos nesant pareiškėjos valios (t. y. pareiškėja siekė, kad mokėjimo operacijų metu lėšos būtų pervestos į jos pačios kitą mokėjimo sąskaitą, tačiau jos buvo pervestos į trečiųjų asmenų sąskaitas) ir buvo inicijuotos trečiųjų asmenų, todėl jos laikytinos neautorizuotomis.

Siekiant išspręsti tarp pareiškėjos ir banko kilusį ginčą bei pasisakyti dėl pareiškėjos keliamų reikalavimų pagrįstumo, Lietuvos banko vertinimu, būtina nustatyti, ar dėl neautorizuotų mokėjimo operacijų bankas privalo pareiškėjai kompensuoti jos patirtus nuostolius.

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

Mokėjimų įstatymo 39 straipsnio 1 dalis nustato, kad 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 pirmiau 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 įrodymų dėl mokėtojo sukčiavimo (nesąžiningumo arba tyčios) arba didelio neatsargumo (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 mokėjimo operacijų įvykdymu, ir ar galėtų pareiškėjos atžvilgiu būti taikoma Mokėjimų įstatymo 39 straipsnio 3 dalis, būtina nustatyti, ar pareiškėjos elgesys, atskleidžiant tam tikrus personalizuotus mokėjimo priemonės (prisijungimo prie banko programėlės naršyklės versijos ir vienkartinius saugos kodus, kurie buvo skirti mokėjimo operacijoms tvirtinti) požymius ir (ar) kiti veiksmai, dėl kurių galėjo būti įvykdytos mokėjimo operacijos, vertintini kaip didelis pareiškėjos neatsargumas, dėl kurio visi jos reikalaujami atlyginti nuostoliai turėtų tekti pačiai pareiškėjai.

Antrosios mokėjimo paslaugų direktyvos (toliau – PSD2) 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 taip pat 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 mano, kad nuostolius dėl mokėjimo operacijų pareiškėja patyrė dėl savo didelio neatsargumo, t. y. pareiškėja savo aktyviais veiksmais patvirtindama trečiųjų asmenų prisijungimą prie jos banko sąskaitos bei atlikdama kitus veiksmus, kurių prašė tretieji asmenys, suteikė leidimą tretiesiems asmenims inicijuoti ir atlikti mokėjimo operacijas pareiškėjos vardu.

Vertinamų aplinkybių kontekste visų pirma būtina pažymėti, kad, remiantis pirmiau

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

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, arba būdamas labai neatsargus.

Taigi, banko sprendimas nekompensuoti pareiškėjos nuostolių dėl neautorizuotų mokėjimo operacijų įvykdymo galėtų būti vertinamas kaip pagrįstas tik tada, jeigu būtų įrodyta, kad pareiškėja, atskleisdama tam tikrus personalizuotus savo mokėjimo priemonių saugumo duomenis ir atlikdama tam tikrus veiksmus, suteikė galimybę tretiesiems asmenims prisijungti prie jos atsiskaitomosios sąskaitos per internetinę banko programėlės versiją, leido inicijuoti ir net patvirtino mokėjimo operacijas, t. y. elgėsi itin aplaidžiai – buvo labai neatsargi.

Lietuvos bankas, siekdamas nustatyti, ar pareiškėjos elgesys šiuo atveju gali būti laikomas itin neatsargiu, vertino pareiškėjos elgesį pasitikint gautame pranešime nurodyta informacija, paskambinant pranešime nurodytu telefono numeriu, atliekant visus trečiųjų asmenų nurodytus veiksmus ir atskleidžiant tam tikrus duomenis, taip pat banko veiksmus, kurių jis prevenciškai ėmėsi ir imasi tam, kad atkreiptų pareiškėjos dėmesį dėl galimos sukčiavimo rizikos.

Vertinant pačios pareiškėjos elgesį, svarbu nustatyti, kaip pareiškėja, kaip mokėjimo paslaugų vartotoja, buvo įtikinta atskleisti savo mokėjimo priemonės personalizuotus saugos duomenis, įgalinusius trečiuosius asmenis inicijuoti mokėjimo operacijas.

Lietuvos bankas, įvertinęs pareiškėjos kreipimesi ir banko atsiliepime nurodytas aplinkybes bei kartu su kreipimusi ir atsiliepimu pateiktus duomenis, nustatė, kad prieš mokėjimo operacijų įvykdymą pareiškėja į mobiliojo telefono žinučių srautą gavo trumpąją SMS žinutę, kurioje buvo nurodyta, kad iš jos mokėjimo sąskaitos yra bandoma atlikti mokėjimo operacijas. Žinutėje buvo nurodyta, kad jeigu ne pareiškėja atlieka mokėjimo operaciją, ji turi paskambinti nurodytu telefono numeriu. Pareiškėja paskambino nurodytu telefono numeriu. Pokalbio metu pareiškėja kalbėjo su tariamu banko atstovu, jam pareiškėja savo aktyviais veiksmais suteikė galimybę prisijungti prie jos asmeninės banko sąskaitos per internetinę banko programėlės versiją, t. y. suvedė PIN kodą tam, kad tretieji asmenys galėtų prisijungti prie jos asmeninės sąskaitos, bei atliko kitus trečiųjų asmenų nurodytus veiksmus, kurie, kaip paaiškėjo vėliau, leido tretiesiems asmenims inicijuoti ir patvirtinti mokėjimo operacijas.

Kaip jau buvo minėta pirmiau, Mokėjimų įstatymo 34 straipsnyje reglamentuojama viena iš mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigų – naudotis mokėjimo priemone pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas. Banko privatiems klientams taikomų mokėjimo paslaugų teikimo sąlygų (toliau – Sąlygos) 9 punkte nustatyta, kad „darome viską, ką galime, kad apsaugotume jūsų pinigus. To paties prašome ir jūsų – saugoti savo saugumo informaciją ir „Revolut" kortelę. […] Savo saugumo informacijos nepateikite niekam kitam, išskyrus atvirosios bankininkystės paslaugų teikėją ar trečiosios šalies teikėją, besilaikantį teisės aktų reikalavimų. Daugiau apie atvirosios bankininkystės paslaugų teikėjus ir trečiosios šalies teikėjus paaiškinome šių nuostatų ir sąlygų 10 skyriuje. Kartais lengva užmiršti veiksmus, kuriuos privalote atlikti, kad apsaugotumėte savo pinigus. Keletas patarimų, kaip juos apsaugoti: būtinai uždarykite „Revolut" programėlę, kai ja nesinaudojate; saugokite savo mobilųjį telefoną ir el. pašto paskyrą ir neleiskite kitiems jais naudotis. Jei jūsų „Revolut" kortelė buvo prarasta ar pavogta arba, jei jūsų „Revolut" kortele ar saugumo informacija kažkas galėjo pasinaudoti be jūsų leidimo, susisiekite su mumis per „Revolut" programėlę."

Taigi, pirmiau aptartos mokėjimo kortelės sutarties (ją sudarančių dokumentų) nuostatos aiškiai nustato, kad už mokėjimo ir tapatybės patvirtinimo priemonių personalizuotų saugumo duomenų konfidencialumą yra atsakingas mokėtojas, šiuo atveju – pareiškėja, ji privalo saugoti jos turimą saugumo informaciją, kad ji netaptų žinomą tretiesiems asmenims. Atsižvelgiant į tai, manytina, kad pareiškėjos elgesys būtų laikomas kaip atitinkantis mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, jei būtų nustatyta, kad pareiškėja ėmėsi adekvačių veiksmų (arba priešingai – nustačius, kad nuo tam tikrų veiksmų susilaikė) tam, kad jai banko išduotų mokėjimo priemonių personalizuotų saugumo duomenų, įgalinančių inicijuoti ir tvirtinti mokėjimus, konfidencialumas būtų tinkamai užtikrintas.

Vis dėlto, įvertinus ginčo byloje esančius duomenis ir ginčo nagrinėjimo metu nustatytas aplinkybes, išvados, kad pareiškėjos elgesys atitiko banko nustatytas naudojimosi mokėjimo priemonėmis sąlygas ir buvo adekvatus, pakankamas tam, kad pareiškėjai nustatytos pareigos, susijusios su mokėjimo priemonių personalizuotų saugumo duomenų konfidencialumo užtikrinimu, būtų tinkamai įvykdytos, daryti negalima.

Nors pareiškėjai į banko žinučių srautą atsiųstos trumposios SMS žinutės pranešimas, kuris informavo pareiškėją, jog jos mokėjimo sąskaitoje galimai yra atliekamos mokėjimo operacijos, galėjo sukurti pirminį įspūdį, kad šis pranešimas yra išsiųstas banko darbuotojo, tačiau tai, kad pareiškėja paskambino trečiajam asmeniui, nedvejodama pasitikėjo juo, leido jam prisijungti prie pareiškėjos atsiskaitomosios sąskaitos, ignoravo jai siunčiamus įspėjamuosius pranešimus ir perdavė tik pareiškėjai siųstus bei žinomus vienkartinius saugos kodus, leidžia teigti, kad pareiškėjos elgesys nebuvo itin apdairus ir atsargus.

Visų pirma svarbu atkreipti dėmesį į tai, kad pareiškėjos itin neatsargus elgesys pasireiškė tada, kai pareiškėja suteikė galimybę tretiesiems asmenims prisijungti prie internetinės banko programėlės versijos.

Iš banko pateiktų duomenų matyti, kad trečiųjų asmenų prisijungimas prie internetinės banko programėlės versijos vyko įvedus pareiškėjos telefono numerį, kuris buvo pateiktas bankui atidarant mokėjimo sąskaitą, o vėliau buvo patvirtintas pareiškėjos mobiliajame telefone įvedus 4 skaitmenų slaptažodį[4].

Pareiškėjai įvedus slaptažodį, jos mobiliajame įrenginyje pasirodė iššokantis pranešimas, kuriame pareiškėja buvo informuojama apie bandymą prisijungti prie jos paskyros, ir buvo prašoma patvirtinti, kad tai norėjo atlikti pareiškėja[5]. Pareiškėjai paspaudus iššokantį pranešimą, pareiškėjos mobiliajame įrenginyje atsidarė autorizacijos langas, kuriame buvo atitinkamo pobūdžio informacija, leidžianti identifikuoti siekiančio prisijungti asmens vietą, naršyklę ir IP adresą. Taip pat pareiškėjai buvo matomas tekstas, kad yra mėginama prisijungti prie pareiškėjos asmeninės mokėjimo sąskaitos per internetinę banko programėlės versiją, bei prašoma patvirtinti, ar tai daro pareiškėja. Galiausiai nurodoma, kad jeigu tai atlieka ne pareiškėja, toks prašymas turėtų būti atšauktas ir apie tai pareiškėja turėtų informuoti banką[6]. Iš banko pateiktų duomenų matyti, kad pareiškėja šiuo atveju pasirinko patvirtinti prisijungimą, todėl įrenginys, iš kurio buvo bandoma prisijungti, buvo pridėtas į įrenginių sąrašą kaip antrinis įrenginys.

Galiausiai, pareiškėjai patvirtinus trečiųjų asmenų prisijungimą prie jos asmeninės sąskaitos, jos mobiliajame įrenginyje pasirodė ir trečias pranešimas, kuris informavo, kad prie pareiškėjos sąskaitos buvo prisijungta iš naujo įrenginio, todėl jeigu tai padarė ne pareiškėja, ji turėtų pakeisti prisijungimo slaptažodį ir susisiekti su banku[7].

Lietuvos banko vertinimu, nagrinėjamu atveju visuose trijuose pareiškėjai siųstuose pranešimuose buvo aiškiai prašoma patvirtinti, kad būtent pareiškėja, o ne tretieji asmenys siekia prisijungti prie pareiškėjos asmeninės sąskaitos per internetinę banko programėlės naršyklės versiją. Tačiau pareiškėja nebuvo pakankamai atidi ir rūpestinga, ignoravo jai siunčiamus pranešimus, suvedė tik jai žinomą 4 skaitmenų PIN kodą ir taip savo aktyviais veiksmai leido tretiesiems asmenims prisijungti prie jos asmeninės sąskaitos per internetinę banko programėlės naršyklės versiją.

Svarbu pažymėti ir tai, kad iš banko pateiktų duomenų matyti, jog, tretiesiems asmenims prisijungus prie pareiškėjos asmeninės sąskaitos per internetinę banko programėlės versiją ir norint inicijuoti mokėjimo operacijas reikėjo suvesti naudos gavėjų duomenis (vardą, pavardę, banko kodą ir banko sąskaitos numerį). Teisingai įvedus naudos gavėjų duomenis ir inicijavus mokėjimo operacijas per internetinę banko programėlės versiją, jie naršyklėje turėjo būti patvirtinti į pareiškėjos mobilųjį telefoną, kuris buvo pateiktas mokėjimo sąskaitos banke atidarymo metu, išsiųstais vienkartiniais saugos kodais. Neįvedę šių vienkartinių saugos kodų, tretieji asmenys nebūtų turėję galimybės patvirtinti inicijuotų mokėjimo operacijų.

Bankas pateikė duomenis, kad į pareiškėjos mobilųjį telefono numerį trumposiomis SMS žinutėmis buvo išsiųsti vienkartiniai slaptažodžiai, kurie buvo skirti mokėjimo operacijoms patvirtinti[8]. Taip pat bankas pateikė duomenis, kurie patvirtina, kad mokėjimo operacijos buvo patvirtintos, t. y. internetinėje banko programėlės versijoje visų mokėjimo operacijų metu buvo suvesti tik pareiškėjai siųsti ir žinomi vienkartiniai saugos kodai. Lietuvos banko vertinimu, šios aplinkybės suponuoja išvadą, kad būtent pareiškėja tretiesiems asmenims turėjo atskleisti į jos mobilųjį telefoną atsiųstus vienkartinius saugos kodus ir taip tretieji asmenys turėjo galimybę

---

[4] Iš banko pateiktų duomenų matyti, kad 4 skaitmenų PIN kodas buvo suvestas iš pareiškėjos mobiliojo įrenginio Iphone 8 Plus, kuriuo pareiškėja naudojosi prieš ir po mokėjimo operacijų atlikimo.

[5] Pareiškėjai rodomos žinutės tekstas: *„There was an attempted web access request. Tap to confirm this was you*".

[6] Pareiškėjai rodomas žinutės tekstas: *„Someone`s trying to log in to your account on the Revolut website. If it`s you, approve it. If it`s not you, reject it, and let us know, as your account may be at risk*".

[7] Pareiškėjai rodomos tekstas: *„We`ve noticed a login attemt to your account from new device. If it wasn`t you, please change your passcode and contact support immediately*".

[8] Vienkartinių saugos žinučių tekstas: *„XXX-XXX is your Revolut authentication code to send [name] X amount*".

patvirtinti inicijuotas mokėjimo operacijas.

Taigi, vertinant pareiškėjos elgesį būtent nagrinėjamo ginčo aplinkybių ir prieš pareiškėją nukreiptos sukčiavimo atakos kontekste, esminėmis aplinkybėmis, vertinant pareiškėjos neatsargumo laipsnį, Lietuvos banko vertinimu, laikytina tai, kad pareiškėjai nesukėlė jokių įtarimų tai, kad jos yra prašoma atlikti veiksmus ir pateikti visus mokėjimo operacijoms patvirtinti reikalingus duomenis, kuriuos pati pareiškėja paaiškinimuose bankui nurodė pateikusi tretiesiems asmenims. Kaip minėta, pagal banko mokėjimo paslaugų teikimo sąlygas, personalizuotų saugumo duomenų pateikimas minėtose sąlygose numatytais atvejais laikomas kliento (šiuo atveju – pareiškėjos) sutikimu įvykdyti mokėjimo operaciją, lėšas nurašant iš kliento (šiuo atveju – pareiškėjos) sąskaitos.

Be to, iš pateiktų duomenų matyti, kad bankas dėjo pastangas tam, kad pareiškėja būtų informuota apie galimą sukčiavimo riziką. Svarbu pažymėti tai, kad tretieji asmenys, inicijuodami mokėjimo operacijas, nurodė, jog mokėjimai yra atliekami pareiškėjai, t. y. mokėjimo operacijų metu naudos gavėja buvo nurodyta pareiškėja, tačiau mokėjimo operacijos buvo atliekamos į kitų naudos gavėjo sąskaitas kituose bankuose. Bankas ginčo Lietuvos banke nagrinėjimo metu pateikė duomenis, jog jo saugos sistemos nustatė, kad mokėjimo operacijų metu lėšų gavėjų duomenys neatitiko realių naudos gavėjų sąskaitoje nurodytų duomenų. Dėl šios priežasties pareiškėjos mobiliajame įrenginyje buvo parodytas pranešimas, kad nesutampa mokėjimo gavėjo vardas su sąskaitos numeriu (angl. *confirmation of payee*), taip pat buvo prašoma patikrinti šią informaciją ir inicijuotas mokėjimo operacijas tęsti tik tada, jeigu pareiškėja yra tikra, kad mokėjimo operacijų gavėjas yra patikimas. Tačiau iš banko pateiktų duomenų matyti, kad pareiškėja ignoravo atsiųstus pranešimus ir vis tiek atlikto tolimesnius veiksmus tam, kad mokėjimo operacijos būtų atliktos.

Taip pat iš banko pateiktų duomenų matyti, kad, pareiškėjai atliekant pirmąsias mokėjimo operacijas naujiems naudos gavėjams, buvo nurodoma, kad mokėjimo operacijos gali būti atliekamos sukčiams, todėl pareiškėja turėjo nurodyti mokėjimo operacijos paskirtį, t. y. pasirinkti vieną iš šešių pateiktų mokėjimo operacijos paskirties pasirinkčių. Iš banko pateiktų paaiškinimų matyti, kad pareiškėja 5 kartus pasirinko „*Payment for Goods and services*“, t. y. „Mokėjimas už prekes ir paslaugas“, ir vieną kartą „*Investment*“, t. y. „Investavimas“, mokėjimo operacijų paskirtį. Po šių atliktų veiksmų pareiškėjai buvo išsiųsti papildomi pranešimai, kurie įspėjo apie galimą sukčiavimo ataką. Svarbu pažymėti tai, kad į pareiškėjos mobiliųjį įrenginį papildomai buvo išsiųsti pranešimas, kad pareiškėja turi būti itin budri, ir buvo pateikti tolimesni galimi variantai: 1) susipažinti su visuotinai paplitusiu bei vykdomu sukčiavimo aferų aprašymais banko interneto tinklalapyje; 2) pasikonsultuoti dėl atliekamo mokėjimo su banko klientų aptarnavimo specialistais; 3) nutraukti inicijuoto mokėjimo vykdymą; 4) nepriklausomai nuo visų įspėjimų ir pareiškėjai suprantant ir sąmoningai prisiimant riziką bei su ja susijusius galimus neigiamus padarinius, patvirtinti ir įvykdyti inicijuoti mokėjimą. Iš banko pateiktų duomenų matyti, kad pareiškėja pasirinko patvirtinti mokėjimo operacijas.

Lietuvos banko vertinimu, minėti duomenys patvirtina, kad bankas, būdamas savo srities profesionalas, dėjo pastangas tam, kad pareiškėja įvertintų aplinkybes ir, jeigu abejoja, nepatvirtintų mokėjimo operacijų tretiesiems asmenims, tačiau pareiškėja nebuvo pakankamai atidi ir rūpestinga, ignoravo minėtus pranešimus ir patvirtino mokėjimo operacijas. Dėl šios priežasties manytina, kad tai tik patvirtina, jog bankas visus veiksmus atliko tinkamai, o pareiškėja elgėsi itin neapdairiai ir nerūpestingai ir neatsižvelgė į pateikiamus pranešimus.

Išanalizavęs šias bei visas kitas ginčo nagrinėjimo metu nustatytas aplinkybes ir ginčo byloje esančius duomenis, Lietuvos bankas daro išvadą, kad vis dėlto šiuo konkrečiu atveju vertinti pareiškėjos elgesio kaip atsargaus ir apdairaus ar tik neatsargaus nėra galima.

Kaip matyti iš nustatytų aplinkybių, mokėjimo operacijas tretieji asmenys be pareiškėjos žinios galėjo atlikti tik dėl to, kad pareiškėja, būdama labai neatsargi, netinkamai įvykdė Mokėjimų įstatyme (34 straipsnis) ir su banku sudarytoje sutartyje įtvirtintus saugaus naudojimo reikalavimus. Taip pat pareiškėja, neįvertinusi jai siunčiamų pranešimų turinio, ir toliau atliko veiksmus, kurie turėjo tiesioginės įtakos mokėjimo operacijoms inicijuoti ir patvirtinti.

Konstatavus, kad pareiškėja, nesilaikydama jai, kaip mokėtojai, Mokėjimų įstatyme ir sutartyje su banku nustatytų pareigų, susijusių su išduotomis mokėjimo priemonėmis, elgėsi labai neatsargiai, kartu darytina išvada, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, nustatančią, kad tokiu atveju mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai.

Dėl šios priežasties, Lietuvos banko vertinimu, bankas neturi pareigos grąžinti (kompensuoti) pareiškėjai neautorizuotų mokėjimo operacijų lėšų, o pareiškėjos bankui keliamas reikalavimas grąžinti ir (arba) kompensuoti mokėjimo operacijų sumą yra nepagrįstas, todėl atmestinas.

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 tapataus ginčo dalyko 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