LIETUVOS BANKO FINANSŲ RINKŲ PRIEŽIŪROS TARNYBOS TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

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

2022-04-20 Nr. 429-137
Vilnius

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

Nustatyta:

2021 m. gruodžio 24 d. pareiškėjui bendrovės išduota mokėjimo kortele panaudojant *Apple Pay* mokėjimo nurodymo patvirtinimo metodą buvo įvykdytos keturios mokėjimo operacijos po 117,68 JAV dolerio laikotarpiu nuo 17:44 val. iki 17:47 val. gavėjui *Codesdirect (*toliau – gavėjas*)* (toliau – mokėjimo operacijos). Bendra mokėjimo operacijų suma – 470,72 JAV dolerio.

2021 m. gruodžio 24 d. pareiškėjas kreipėsi į bendrovę ir nurodė, kad neatpažįsta pasinaudojant jam priklausančia mokėjimo kortele inicijuotų mokėjimo operacijų. Pareiškėjas bendrovei teigė, kad mokėjimo kortelė buvo jo žinioje – jos jis nebuvo praradęs ir niekam kitam nebuvo perdavęs.

Atlikusi tyrimą bendrovė priėmė sprendimą atsisakyti pareiškėjui grąžinti jo mokėjimo operacijų sumą, nes bendrovė nerado jokių apgaulingos veiklos požymių, dėl to, bendrovės nuomone, pats pareiškėjas yra atsakingas už atliktas mokėjimo operacijas.

Pareiškėjas nesutiko su bendrovės sprendimu, todėl per savo atstovą kreipėsi į Lietuvos banką dėl vartojimo ginčo nagrinėjimo. Kreipimesi pareiškėjo atstovas nurodė, kad pareiškėjas tapo neteisėtų trečiųjų asmenų veiksmų auka, nes iš pareiškėjo sąskaitos bendrovėje panaudodami pareiškėjui priklausančią mokėjimo kortelę tretieji asmenys įvykdė mokėjimo operacijas, nors jų atlikti pareiškėjas nedavė sutikimo. Pareiškėjo atstovas paaiškino, kad tada, kai mokėjimo operacijos buvo atliekamos, pareiškėjas kartu su juo buvo kino teatre, žiūrėjo filmą, taigi, tuo metu pareiškėjas nesinaudojo nei telefonu, nei interneto ryšiu. Pareiškėjo atstovas paaiškino, kad pareiškėjas į savo telefoną gavo SMS žinutę su vienkartiniu saugos kodu, skirtu mokėjimo kortelei prie *Apple Pay* pridėti, tačiau dėl to, kad buvo prastas tiek telefono, tiek interneto ryšys, pareiškėjas gautą SMS žinutę perskaitė tik išėjęs iš kino teatro, būtent tada ir pamatė iš jo sąskaitos įvykdytas neautorizuotas mokėjimo operacijas. Pareiškėjo atstovas paaiškino, kad SMS žinute gauto vienkartinio saugos kodo, kuriuo buvo patvirtintas mokėjimo kortelės pridėjimas prie *Apple Pay*, pareiškėjas niekam neatskleidė.

Bendrovė Lietuvos bankui pateiktame atsiliepime nurodė, kad nesutinka tenkinti pareiškėjo reikalavimo. Bendrovė paaiškino, kad išanalizavusi vidinės kontrolės sistemos duomenis nustatė, kad mokėjimo operacijos buvo atliktos panaudojant bekontaktį mokėjimo metodą – prie *Apple Pay* sistemos buvo pridėta pareiškėjo mokėjimo kortelė. Bendrovė pažymėjo, kad, norėdamas pridėti mokėjimo kortelę prie *Apple Pay* sistemos, kuria siekiama atlikti mokėjimo operacijas, mokėjimo kortelės turėtojas turi suvesti mokėjimo kortelės duomenis (mokėjimo kortelės numerį, kortelės saugos kodą (CVV) ir papildomai patvirtinti mokėjimo kortelės pridėjimą prie *Apple Pay* sistemos įvedant vienkartinį saugos kodą, kurį mokėjimo kortelės savininkas gauna SMS žinute. Minėta žinutė su vienkartiniu saugos kodu visais atvejais yra siunčiama į telefono numerį, kuris buvo nurodytas ir autorizuotas vartotojo sudarant sutartį su bendrove.

Pareiškėjas patvirtino, kad jo mokėjimo kortelė buvo jo žinioje ir kad niekam kitam jis

jos nebuvo perdavęs. Be to, bendrovės teigimu, net ir tuo atveju, jeigu mokėjimo kortelės duomenys būtų atskleisti ar įgyti be mokėjimo kortelės savininko žinios, praktiškai yra neįmanoma, kad trečioji šalis be kortelės savininko žinios galėtų gauti ir vienkartinį saugos kodą, kuris SMS žinute buvo išsiųstas į pareiškėjo telefono numerį. Bendrovės manymu, atsižvelgiant į tai, kad mokėjimo operacijų autentiškumo patvirtinimo procedūra buvo atlikta tinkamai, tikėtina, kad, jeigu mokėjimo operacijas inicijavo ne pats pareiškėjas, tuomet dėl jo netinkamo elgesio jo mokėjimo kortelės duomenys bei SMS žinute gautas vienkartinis saugos kodas buvo atskleistas tretiesiems asmenims. Bendrovė paaiškino, kad Mokėjimų įstatymo 34 straipsnyje nustatyta mokėtojo pareiga gavus mokėjimo priemonę imtis veiksmų, kad būtų apsaugoti personalizuoti saugumo duomenys, o sužinojus apie mokėjimo priemonės praradimą, vagystę arba neteisėtą pasisavinimą ar neautorizuotą jos naudojimą, nedelsiant apie tai pranešti mokėjimo paslaugų teikėjui arba jo nurodytam subjektui. Analogiškos pareigos nustatytos ir bendrovės ir pareiškėjo sudarytos paslaugų teikimo sutarties 9 dalyje: „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. <...>"

Bendrovė pažymėjo, kad mokėjimo kortelė prie *Apple Pay* sistemos buvo pridėta 15:39:54 val. ir pirmoji mokėjimo operacija buvo atlikta 17:43 val., taigi, jeigu *Apple Pay* patvirtinimo kodo informacija nebūtų buvusi atskleista trečiajai šaliai, pridėti kortelės prie *Apple Pay*, esančios kitame neatpažintame įrenginyje, yra faktiškai neįmanoma. Bendrovė taip pat pažymėjo, kad jos vidinių sistemų duomenys neužfiksavo mėginimo prie pareiškėjo sąskaitos jungtis iš kito, ne pareiškėjui priklausančio įrenginio.

Bendrovė teigia, kad iš turimų duomenų galima daryti pagrįstą išvadą, kad mokėjimo operacijos negalėjo būti atliktos sukčių, nes buvo inicijuotos panaudojant *Apple Pay*, o mokėjimo kortelė ir mobilusis įrenginys inicijuojant mokėjimo operacijas buvo pareiškėjo žinioje.

Kadangi, bendrovės turimais duomenimis, mokėjimo kortelė buvo pridėta prie *Apple Pay* sistemos ir buvo suvestas vienkartinis SMS žinute į pareiškėjo telefono numerį gautas saugos kodas, bendrovė teigia, kad negali tenkinti pareiškėjo prašymo grąžinti mokėjimo operacijų lėšas, ir prašė pareiškėjo reikalavimą bendrovei grąžinti mokėjimo operacijų lėšas laikyti nepagrįstu.

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. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą ir jo pagrindu priimamas sprendimas.

Pareiškėjo ir bendrovės ginčas kilo dėl bendrovės atsisakymo grąžinti pareiškėjui pareiškėjo mokėjimo kortele panaudojant *Apple Pay* mokėjimo metodą atliktų mokėjimo operacijų, kurių bendra vertė – 470,72 JAV dolerio ir kurių atlikti pareiškėjas teigia nedavęs sutikimo, sumą.

Pareiškėjas teigia nedavęs sutikimo įvykdyti mokėjimo operacijų, o lėšos iš jo mokėjimo kortelės sąskaitos buvo nurašytos dėl to, kad tretieji asmenys pasisavino pareiškėjo mokėjimo kortelės duomenis, todėl bendrovė turi grąžinti pareiškėjui šių mokėjimo operacijų sumą. Bendrovė teigia, kad mokėjimo operacijos buvo įvykdytos panaudojant *Apple Pay* mokėjimo metodą. Bendrovės teigimu, jos sistemų duomenys patvirtina, kad pareiškėjo mokėjimo kortelė buvo priregistruota prie *Apple Pay* panaudojant mokėjimo kortelės duomenis (kortelės numerį, CVV kodą) bei kortelės pridėjimą patvirtinant pareiškėjo sutartyje nurodytu telefono numeriu bendrovės išsiųstoje žinutėje pateiktu vienkartiniu saugos kodu. Bendrovės teigimu, mokėjimo operacijas autorizavo arba pats pareiškėjas, arba pareiškėjas dėl didelio neatsargumo atskleidė tretiesiems asmenis mokėjimo kortelės duomenis bei vienkartinį saugos kodą, dėl to tretieji asmenys galėjo įgyti galimybę, pasinaudojant pareiškėjo dėl didelio neatsargumo atskleistais duomenimis, inicijuoti ginčijamas mokėjimo operacijas.

Siekiant išspręsti tarp pareiškėjo ir bendrovės kilusį ginčą, Lietuvos banko vertinimu,

būtina nustatyti, ar ginčijamos mokėjimo operacijos laikytinos autorizuotomis ir ar bendrovė turėjo (turi) pareigą grąžinti pareiškėjui ginčijamų mokėjimo operacijų 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.

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 jo mokėjimo paslaugų teikėjo sudaromoje bendrojoje mokėjimo paslaugų teikimo sutartyje (toliau – bendroji sutartis).

Bendrovės ir pareiškėjo sudarytos bendrosios paslaugų teikimo privatiems klientams sutarties 14 punkte pareiškėjas ir bendrovė buvo sutarę, kad mokėjimai gali būti autorizuojami įvedant mokėjimo kortelės duomenis (kortelės numerį, galiojimo datą, CVV kodą) arba PIN kodą. Šiuos veiksmus bendrovė laiko mokėtojo sutikimu atlikti mokėjimus iš bendrovės sąskaitos (angl. *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*).

Atsižvelgiant į tai, kad bendroji sutartis nustato bendrovės ir pareiškėjo tarpusavio santykius, bei 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, pareiškėjo ir bendrovės 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.

Bendrovė Lietuvos bankui pateikė sistemų duomenis, kurie patvirtina, kad mokėjimo operacijos kortele buvo inicijuotos pasinaudojant *Apple Pay* mokėjimo metodu. Tam, kad būtų galima atsiskaityti pasinaudojant *Apple Pay* mokėjimo metodu, būtina mokėjimo kortelę pridėti prie *Apple Pay* sistemos. Mokėjimo kortelei prie *Apple Pay* sistemos pridėti yra taikoma saugesnio autentiškumo patvirtinimo procedūra, kurios metu reikia ne tik pateikti mokėjimo kortelės duomenis, bet ir suvesti vienkartinį saugos kodą. Pareiškėjas neginčija, kad į savo telefono numerį gavo SMS žinutę su vienkartiniu saugos kodu, skirtu mokėjimo kortelei prie *Apple Pay* pridėti, be to, jo paties pateiktas bendrovės gautų SMS žinučių išrašas patvirtina, kad 2021 m. gruodžio 24 d. 15:39 val. pareiškėjas į savo telefono numerį gavo bendrovės SMS žinutę su vienkartiniu saugos kodu, skirtu mokėjimo kortelės pridėjimui prie *Apple Pay* sistemos patvirtinti. Kita vertus, pareiškėjas teigė, kad nei savo mokėjimo kortelės, nei savo telefono aparato nebuvo pametęs ir (arba) perdavęs tretiesiems asmenims, juos turėjo su savimi. Taigi, nors ir teigia, kad tiek mokėjimo kortelė, tiek telefono aparatas inicijuojant mokėjimo operacijas visą laiką buvo jo žinioje, tačiau neigia pats inicijavęs mokėjimo operacijas gavėjui ir mano, kad tai buvo padaryta dėl neteisėtų trečiųjų asmenų veiksmų. Bendrovė nurodė, kad jokių techninių trikdžių atliekant ginčijamas mokėjimo operacijas nebuvo užfiksuota, taip pat nebuvo užfiksuota jokių trečiųjų asmenų įsilaužimo į pareiškėjo mokėjimo kortelės sąskaitą bendrovės programėlėje požymių.

Įvertinus pareiškėjo paaiškinimus apie mokėjimo operacijų atlikimo aplinkybes bei surinktus duomenis iš bendrovės sistemų, jeigu darytume prielaidą, kad mokėjimo operacijas galėjo inicijuoti ne pats pareiškėjas, o tretieji asmenys be pareiškėjo žinios ir sutikimo, tuomet tam, kad tretieji asmenys be pareiškėjo žinios ir sutikimo galėtų inicijuoti mokėjimo operacijas, jie turėtų turėti arba pareiškėjo mokėjimo kortelės duomenis bei SMS žinute pareiškėjui telefonu bendrovės atsiųstą vienkartinį saugos kodą, arba pareiškėjo telefono įrenginį su prisijungimo prie *Apple Pay* duomenimis. Kaip ir minėta, pareiškėjas neginčija, kad iš bendrovės SMS žinute į savo telefono numerį gavo vienkartinį saugos kodą, skirtą kortelės pridėjimui prie

Apple Pay patvirtinti, ir teigia šio kodo niekam neatskleidęs ir niekam nebuvo perdavęs savo mokėjimo kortelės ir telefono įrenginio. Vadinasi, tiek mokėjimo priemonė, tiek mokėjimo operacijoms autorizuoti reikalingi personalizuoti saugos duomenys inicijuojant mokėjimo operacijas buvo tik pareiškėjo žinioje.

Taigi, įvertinus turimus duomenis, būtent tai, kad, bendrovės pateiktais duomenimis, nebuvo užfiksuota jokių trečiųjų asmenų neteisėtų veiksmų pareiškėjo bendrovės turimoje sąskaitoje, tai, kad pareiškėjas teigė, jog mokėjimo kortelės nebuvo pametęs ir niekam nebuvo jos perdavęs, bei faktą, kad pats pareiškėjas pateikė informaciją, kad iš bendrovės gavo SMS žinutę su vienkartiniu saugos kodu, skirtu mokėjimo kortelės pridėjimui prie *Apple Pay* patvirtini, ir neginčijo, kad pats savo mokėjimo kortelę pridėjo prie *Apple Pay*, taip pat tai, kad pareiškėjas teigė, kad niekam neatskleidė SMS žinute gauto vienkartinio saugos kodo ir kad nebuvo praradęs savo telefono įrenginio ir visą laiką turėjo su savimi, yra pagrindas vertinti, kad mokėjimo kortelę prie *Apple Pay* pridėjo ne tretieji asmenys be pareiškėjo žinios ir sutikimo, o pats pareiškėjas. Taip pat, bendrovės pateiktais duomenimis, bendrovė neužfiksavo prisijungimo prie pareiškėjo sąskaitos bendrovėje iš kito, ne pareiškėjui priklausančio, įrenginio.

Ginčo byloje taip pat nėra nustatyta jokių neteisėtų trečiųjų asmenų veiklos požymių, kad tretieji asmenys galėjo pasisavinti pareiškėjo mokėjimo kortelės duomenis bei vienkartinį saugos kodą ir be pareiškėjo žinios ir sutikimo inicijuoti mokėjimo operacijas, todėl nėra pagrindo vertinti pareiškėjo kaltės formos, t. y. vertinti, ar pareiškėjas mokėjimo priemonę prarado tyčia, ar dėl didelio neatsargumo neįvykdęs vienos ar kelių Mokėjimų įstatymo 34 straipsnyje nustatytų pareigų.

Nors pareiškėjas teigia pats neinicijavęs mokėjimo operacijų, tačiau tvirtina, kad mokėjimo kortelė visą laiką buvo jo žinioje ir niekam nebuvo jos perdavęs, ir iš esmės neginčija, kad prie *Apple Pay* sistemos pridėjo savo mokėjimo kortelę. Vis dėlto iš pareiškėjo pateikto ginčo aplinkybių aiškinimo galima manyti, kad pareiškėjas nevisiškai suprato *Apple Pay* mokėjimo metodo veikimo principą, t. y. pareiškėjas galbūt nesuprato, kad mokėjimo operaciją inicijuojant *Apple Pay* mokėjimo metodu bendrovė papildomai SMS žinute nesiunčia papildomo vienkartinio saugos kodo, kad būtų patvirtinta konkreti mokėjimo operacija. Šiuo atveju mokėtojo sutikimas įvykdyti konkrečią mokėjimo operaciją naudojant *Apple Pay* metodą yra duodamas mokėjimo kortelę pridedant prie *Apple Pay*. Mokėjimo kortelę pridėjus prie *Apple Pay* sistemos ir pridėjimą patvirtinus saugos kodu, yra įgyjama galimybė naudotis mokėjimo kortele kaip sava, jos fiziškai neturint. Kaip ir buvo minėta, mokėjimo kortelės pridėjimui prie *Apple Pay* buvo taikyta saugesnio autentiškumo patvirtinimo procedūra. Bendrovės Lietuvos bankui pateikti duomenys patvirtina, kad visos mokėjimo operacijos buvo įvykdytos pasinaudojant pareiškėjo mokėjimo kortele panaudojant *Apple Pay* metodą.

Kaip ir buvo minėta, pareiškėjui teigiant, kad jis neprarado mokėjimo kortelės bei niekam neatskleidė bendrovės pareiškėjo ir bendrovės sutartyje nurodytu telefono numeriu išsiųsto vienkartinio saugos kodo, skirto mokėjimo kortelės pridėjimui prie *Apple Pay* patvirtinti, esant objektyvių duomenų, kad pareiškėjo mokėjimo kortelė prie *Apple Pay* sistemos buvo pridėta laikantis saugesnio autentiškumo patvirtinimo reikalavimų, taip pat atsižvelgiant į tai, kad pareiškėjo ir bendrovės sutartyje buvo sutarta dėl mokėjimo operacijų kortele autorizavimo tvarkos, kaip yra pateikiami mokėjimo kortelės duomenys ir (arba) PIN kodo slaptažodis, taip pat nesant jokių objektyvių duomenų, kad tretieji asmenys neteisėtu būdu būtų pasisavinę pareiškėjo mokėjimo priemonę, nėra pagrindo vertinti, kad pareiškėjo mokėjimo operacijos gali būti laikomos neautorizuotomis, t. y. įvykdytomis be pareiškėjo žinios ir sutikimo. Atitinkamai darytina išvada, kad bendrovė neturi pareigos pareiškėjui grąžinti mokėjimo operacijų, kurios buvo patvirtintos bendrovės ir pareiškėjo sutartyje sutarta tvarka ir bendrovės tinkamai įvykdytos, lėšų. Atsižvelgiant į tai, darytina išvada, kad pareiškėjo reikalavimas bendrovei grąžinti mokėjimo operacijų sumą – 470,72 JAV dolerio, yra nepagrįstas, todėl atmestinas.

Remdamasis tuo, kas išdėstyta, ir vadovaudamasis 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 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 Lietuvos banko 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