LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

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

2023-09-20 Nr. 429-476
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:

Iš pareiškėjo sąskaitos banke panaudojant pareiškėjui išduotą mokėjimo kortelę 2022 m. gruodžio 22 d. buvo įvykdytos 6 mokėjimo operacijos skirtingiems gavėjams (toliau – gavėjai). Bendra mokėjimo operacijų suma – 3 654,68 GBP (toliau – mokėjimo operacijos). Mokėjimo operacijos buvo patvirtintos *Apple Pay* mokėjimo metodu.

2022 m. gruodžio 23 d. pareiškėjas kreipėsi į banką ir teigė, kad jis neautorizavo mokėjimo operacijų ir kad jos buvo inicijuotos trečiųjų asmenų, kuriems jis padiktavo telefonu SMS žinute gautą vienkartinį saugos kodą, skirtą pridėti mokėjimo kortelę prie *Apple Pay*, įdiegto kitame įrenginyje. Pareiškėjas teigė, kad mokėjimo kortelės duomenų tretiesiems asmenims neatskleidė, ir prašė, kad bankas grąžintų visą neautorizuotų mokėjimo operacijų sumą.

Bankui nesutikus tenkinti pareiškėjo reikalavimo, pareiškėjas dėl vartojimo ginčo nagrinėjimo kreipėsi į Lietuvos banką.

Pareiškėjas kreipimesi į Lietuvos banką teigė, kad jam telefonu paskambino asmenys, apsimetę *Revolut* darbuotojais, ir jį įspėjo, kad kilo problemų jo banko sąskaitos saugumui, nes jo asmeninė informacija, įskaitant ir jo bankininkystės duomenis, buvo paviešinta jam apsiperkant elektroninėje parduotuvėje *Amazon*. Pareiškėjas teigė, kad tretieji asmenys turėjo jo duomenis, todėl sugebėjo pareiškėją įtikinti atskleisti banko jam SMS žinute siųstą vienkartinį saugos kodą. Pareiškėjas teigė, kad šį kodą atskleidė norėdamas patvirtinti savo tapatybę. Pareiškėjas teigia, kad kitą dieną pastebėjo, kad iš jo sąskaitos banke be jo žinios ir sutikimo yra įvykdytos mokėjimo operacijos. Pareiškėjo nuomone, bankas jam kreipusis dėl mokėjimo operacijų atšaukimo, turėjo galimybę jas atšaukti, nes lėšos banko sąskaitoje dar buvo tik rezervuotos.

Bankas nesutinka tenkinti pareiškėjo reikalavimo. Bankas paaiškino, kad pareiškėjo mokėjimo kortelė prie *Apple Pay*, įdiegto kitame įrenginyje, buvo pridėta panaudojus mokėjimo kortelės duomenis bei pareiškėjo telefonu banko SMS žinute siųstą vienkartinį saugos kodą. SMS žinutėje, kurioje buvo pateikiamas vienkartinis saugos kodas, buvo nurodyta ir minėto kodo naudojimo paskirtis – pridėti mokėjimo kortelę prie *Apple Pay*, įdiegto kitame įrenginyje. Pareiškėjas pripažino šį saugos kodą telefonu padiktavęs tretiesiems asmenims. Bankas teigia, kad pareiškėjas dėl savo didelio neatsargumo tretiesiems asmenins perdavė savo mokėjimo priemonės duomenis, tai ir lėmė mokėjimo operacijų įvykdymą iš pareiškėjo banko sąskaitos. Bankas įvykdytas mokėjimo operacijas laiko pareiškėjo autorizuotomis, nes pateikti įrodymai patvirtina, kad pats pareiškėjas tretiesiems asmenims perdavė savo mokėjimo priemonės duomenis.

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.

Ginčas kilo dėl to, kad bankas atsisakė grąžinti pareiškėjui jo mokėjimo kortele, naudojant *Apple Pay* mokėjimo nurodymo patvirtinimo metodą, atliktų mokėjimo operacijų, kurių bendra vertė 3 654,68 GBP, sumą.

Pareiškėjas teigia nedavęs sutikimo atlikti mokėjimo operacijas, neigia jas autorizavęs. Pareiškėjas teigia, kad banko darbuotojais prisistačiusiems asmenims atskleidė SMS žinute gautą vienkartinį saugos kodą ir to pakako, kad tretieji asmenys jo mokėjimo kortelę pridėtų prie *Apple Pay* sistemos. Bankas teigia, kad mokėjimo operacijos buvo įvykdytos naudojant *Apple Pay* mokėjimo nurodymo patvirtinimo metodą. Tam, kad pareiškėjo mokėjimo kortelė būtų pridėta prie *Apple Pay* sistemos, buvo panaudoti pareiškėjo mokėjimo kortelės duomenys, o pridėjimas patvirtintas banko į sutartyje nurodytą telefono numerį išsiųstoje žinutėje pateiktu vienkartiniu saugos kodu. Banko vertinimu, mokėjimo operacijas autorizavo pats pareiškėjas arba pareiškėjas dėl didelio neatsargumo atskleidė tretiesiems asmenims savo mokėjimo kortelės duomenis ir vienkartinį saugos kodą, dėl to tretieji asmenys galėjo įgyti galimybę inicijuoti mokėjimo operacijas *Apple Pay* mokėjimo metodu.

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) mokėjimo operacijos laikytinos autorizuotomis; 2) bankas privalo grąžinti pareiškėjui mokėjimo operacijų sumą.*

1. Dėl mokėjimo operacijų 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 kortele terminalą (bekontaktis atsiskaitymas) ar atliekant kitus veiksmus su elektroniniu kortelių skaitytuvu. Šiuos veiksmus bankas laiko mokėtojo sutikimu atlikti mokėjimus iš banko sąskaitos[1]. 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 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 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.

[1] 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 <…>"*.

Banko kartu su atsiliepimu pateiktais vidaus sistemos duomenimis, visos mokėjimo operacijos atliktos tuo pačiu mobiliuoju įrenginiu su IOS operacine sistema, kuris kaip *Apple Pay* mokėjimo įrenginys prie *Apple Pay* sistemos buvo pridėtas ir autorizuotas 2022 m. gruodžio 22 d.

Pareiškėjas neigia pats autorizavęs mokėjimo operacijas ir kam nors atskleidęs savo mokėjimo kortelės duomenis, tačiau pripažįsta telefonu tretiesiems asmenims atskleidęs SMS žinute gautą vienkartinį saugos kodą.

Vis dėlto, kaip paaiškino bankas atsiliepime, norėdamas pridėti mokėjimo kortelę prie *Apple Pay (ar Android Pay, Garmini Pay)*, asmuo turi atlikti aktyvius veiksmus, numatytus *Apple Pay* sąlygose[2]: 1) įrenginyje, kuriuo siekiama atlikti *Apple Pay* mokėjimą, reikia įvesti mokėjimo kortelės duomenis (kortelės numerį, saugos kodą CVV, kita) arba nuskaityti mokėjimo kortelę; 2) suvedęs mokėjimo kortelės duomenis, asmuo turi perskaityti ir sutikti su mokėjimo sąlygomis; 3) siekdamas patvirtinti mokėjimo kortelės duomenis, 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. Banko pateiktais duomenis, pareiškėjui jo bankui nurodytu telefonu numeriu buvo išsiųsta SMS žinutė su vienkartiniu saugos kodu, tai, banko teigimu, reiškia, kad pirmiau nurodyti veiksmai pareiškėjo mokėjimo kortelei prie *Apple Pay* įrenginio pridėti – pareiškėjo mokėjimo kortelės duomenų (numeris, CVV kodas) suvedimas, taip pat buvo atlikti.

Atsiliepime, net ir atsižvelgdamas į tai, kad mokėjimo operacijos buvo inicijuotos jų įvykdymo dieną, prie *Apple Pay* sistemos pridėjus pareiškėjo mokėjimo kortelę naujame įrenginyje, kuris, kaip teigia bankas, nepriklauso pareiškėjui, bankas teigė, kad šie mokėjimai laikytini autorizuotais, nes mokėjimo kortelė inicijuojant mokėjimus buvo pareiškėjo žinioje, o prie *Apple Pay* sistemos pridėta suvedus į pareiškėjo mobilųjį telefoną SMS žinute atsiųstą vienkartinį saugos kodą.

Vis dėlto, įvertinus pareiškėjo paaiškinimus apie mokėjimo operacijų 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.

Nors, ginčo bylos duomenimis, pareiškėjo mokėjimo kortelė prie *Apple 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, nustatyti ir banko neginčijami duomenys leidžia pagrįstai abejoti, ar mokėjimo priemonė, kuria atliktos mokėjimo operacijos, buvo tik pareiškėjo žinioje. Dėl to, pačiam pareiškėjui neigiant mokėjimų operacijų autorizavimo aplinkybę ir esant pagrįstų duomenų apie įvykusį sukčiavimo atvejį – taigi, kad pareiškėjo mokėjimo priemone ir jo personalizuotais saugumo duomenimis be pareiškėjo žinios ir nesant jo valios galėjo neteisėtai pasinaudoti tretieji asmenys, negalima daryti išvados, kad pareiškėjo mokėjimo kortele atliktos mokėjimo operacijos buvo jo autorizuotos, t. y. inicijuotos ir patvirtintos esant paties pareiškėjo sutikimui, kaip tai suprantama Mokėjimų įstatymo 29 straipsnio 1 dalies kontekste.

Atsižvelgdamas į tai, Lietuvos bankas daro išvadą, kad mokėjimo operacijos laikytinos neautorizuotomis.

2. *Dėl neautorizuotų mokėjimo operacijų pasekmių ir pareiškėjo teisės į mokėjimų operacijų sumos grąžinimą*

Pagal Mokėjimų įstatymo 38 straipsnio 1 dalį, joje nurodytomis sąlygomis ir tvarka mokėtojo mokėjimo paslaugų teikėjas privalo grąžinti 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 nesąžiningai arba tyčia ar dėl didelio neatsargumo neįvykdęs vienos ar kelių šio įstatymo 34 straipsnyje[3] nustatytų pareigų.

---

[2] Add a debit or credit card – Apple Pay Help

[3] 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.

Mokėjimų įstatymas aiškiai nustato, kad tuo atveju, kai mokėtojas neigia autorizavęs įvykdytą mokėjimo operaciją, mokėtojo mokėjimo paslaugų teikėjo arba atitinkamais atvejais mokėjimo inicijavimo paslaugos teikėjo užregistruotas mokėjimo priemonės naudojimas nebūtinai yra pakankamas įrodymas, kad mokėtojas autorizavo mokėjimo operaciją ar veikė nesąžiningai arba tyčia ar dėl didelio neatsargumo neįvykdė vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų. Mokėtojo mokėjimo paslaugų teikėjas ir atitinkamais atvejais mokėjimo inicijavimo paslaugos teikėjas turi pateikti įrodymų, kuriais patvirtinamas mokėtojo sukčiavimas arba didelis neatsargumas (Mokėjimų įstatymo 37 straipsnio 3 dalis).

Įvertinus nurodytas Mokėjimų įstatymo nuostatas, galima teigti, kad mokėtojo mokėjimo paslaugų teikėjas gali būti visiškai atleistas nuo pareigos grąžinti mokėtojui neautorizuotos mokėjimo operacijos sumą tik tuo atveju, jeigu pateikia mokėtojo sukčiavimo (nesąžiningumo arba tyčios) arba didelio neatsargumo įrodymų, t. y. jeigu iš mokėjimo paslaugų teikėjo pateiktų įrodymų nustatoma, kad mokėtojas ne tik neįvykdo vienos ar kelių jam Mokėjimų įstatyme nustatytų pareigų, bet ir padaro tai elgdamasis nesąžiningai arba tyčia ar būdamas labai neatsargus (Mokėjimų įstatymo 37 straipsnio 3 dalis ir 39 straipsnio 3 dalis).

Aplinkybių ir duomenų, kaip ir šalių ginčo dėl to, kad pareiškėjas galėjo veikti nesąžiningai arba tyčia, įskaitant sukčiavimą, nėra. Bankas sprendimą nekompensuoti pareiškėjo nuostolių grindžia vertinimu, kad mokėjimo operacijos buvo autorizuotos 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 mokėjimo operacijų 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 įvykdytos mokėjimo operacijos, 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 pareiškėjo 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.

Vadovaujantis ginčo byloje esančiais banko vidaus sistemų duomenimis, pareiškėjo ginčijamos mokėjimo operacijos buvo įvykdytos mokėjimo kortele, panaudojant *Apple Pay* mokėjimo metodą. Banko teigimu, kad būtų galima atsiskaityti naudojant *Apple Pay* mokėjimo metodą, 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[4], kuris, pagal banko pateiktus įrodymus, šiuo atveju ir buvo suvestas. Bankas nurodė, kad jokių techninių trikdžių atliekant mokėjimo operacijas nebuvo užfiksuota, taip pat nebuvo užfiksuota jokių trečiųjų asmenų įsilaužimo į pareiškėjo mokėjimo kortelės sąskaitą banko programėlėje požymių.

Įrodymų pakankamumas civiliniame procese grindžiamas tikėtinumo taisykle (tikimybių

Mokėjimo paslaugų vartotojas, gavęs mokėjimo priemonę, privalo imtis veiksmų, kad būtų apsaugoti personalizuoti saugumo duomenys (Mokėjimų įstatymo 34 straipsnio 2 dalis).

[4] Pagal pirmiau minėtas *Apple Pay* sąlygas, vienkartinis saugos kodas SMS žinute banko kliento telefono numeriu yra siunčiamas tik tuomet, kai suvedami teisingi mokėjimo kortelės, kurią siekiama pridėti prie *Apple Pay* įrenginio, duomenys.

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[5].

Tad nors pareiškėjas teigė, kad jokių savo mokėjimo priemonės personalizuotų saugumo duomenų ir (ar) kokių nors kitų savo duomenų niekam nėra atskleidęs, o mokėjimo kortelės ir (ar) jos valdymo kontrolės niekada nebuvo praradęs, ginčo byloje nustatyta, kad pareiškėjo mokėjimo kortelė prie *Apple Pay* sistemos naujame įrenginyje galėjo būti pridėta tik suvedus mokėjimo kortelės numerį ir šios kortelės CVC kodą, taip pat, ginčo byloje esančiais įrodymais ir šalių neginčijamomis aplinkybėmis, būtent į pareiškėjo mobilųjį telefoną atsiųstą vienkartinį saugos kodą. Nesant kitų galimybių nustatyti ir (ar) nenustačius kitokias aplinkybes pagrindžiančių duomenų, kaip pareiškėjo mokėjimo priemonių personalizuoti saugumo duomenys be paties pareiškėjo veiksmų galėjo tapti žinomi tretiesiems asmenims, kai, pareiškėjo teigimu, jo mokėjimo kortelė buvo jo žinioje, neginčijant konstatuotos aplinkybės, kad mokėjimo operacijos yra neautorizuotos ir jų įvykdyti savo valia pareiškėjas nesiekė, labiau tikėtina, kad būtent pats pareiškėjas, galbūt nesuprasdamas atliekamų veiksmų reikšmės ir pasekmių, atskleidė tretiesiems asmenims visus duomenis, būtinus jo mokėjimo kortelei pridėti prie *Apple Pay* sistemos naujame įrenginyje, kuriuo vėliau ir buvo patvirtintos visos mokėjimo operacijos.

Taisyklių 45 punktas nustato, kad 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.

Tad nors pareiškėjas neigia atskleidęs tretiesiems asmenims su jo banko mokėjimo kortele susijusius duomenis, vis dėlto nustatytos aplinkybės leidžia konstatuoti priešingai.

Pareiškėjas, pateikdamas paaiškinimus dėl mokėjimo operacijų įvykdymo aplinkybių ir kartu dėl banko atžvilgiu savo keliamo reikalavimo pagrįstumo, nurodė, kad su juo susiekė asmuo, prisistatęs banko darbuotoju, ir nurodė, kad pareiškėjas turi patvirtinti savo tapatybę tam, kad būtų užblokuotas pareiškėjo anksčiau inicijuotas mokėjimo pavedimas. Šiuo tikslu pareiškėjo buvo paprašyta patvirtinti savo tapatybę ir padiktuoti SMS žinute gautą vienkartinį saugos kodą.

Išanalizavęs ginčo byloje esančius duomenis ir kitas nustatytas aplinkybes, Lietuvos bankas mano, kad pareiškėjo elgesys negali būti vertinamas kaip atsargus ir apdairus ar tik neatsargus.

Kaip nustatyta, pridedant pareiškėjo mokėjimo kortelę prie *Apple 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 vienkartiniu saugos kodu pareiškėjui SMS žinutėje buvo nurodyta šio kodo paskirtis ir perspėjimas jo neperduoti tretiesiems asmenims (standartinis siunčiamos SMS žinutės tekstas lietuvių kalba: „Šis kodas bus naudojamas jūsų kortelei pridėti prie kito „Apple Pay" įrenginio. Niekur jo neįveskite, nebent norite pridėti savo kortelę prie naujo įrenginio. Nesidalinkite šiuo kodu su niekuo, net jei jie teigia esantys iš Revolut. „Revolut" patvirtinimo kodas, skirtas „Apple Pay": xxxxxx")[6]. Suvedus gautą vienkartinį saugos kodą, mokėjimo kortelės pridėjimas buvo patvirtintas, o atsiskaitymo *Apple Pay* paslauga aktyvuota – ja naudojantis ir inicijuotos bei patvirtintos visos mokėjimo operacijos.

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, pasitikėjo nepažįstamų jam skambinusių asmenų nurodymais ir atskleidė jiems šį kodą. Jeigu pareiškėjas perskaitė SMS žinutės tekstą, tačiau jame nurodytą vienkartinį saugos kodą vis tiek nusprendė atskleisti tretiesiems asmenims, pareiškėjas taip pat vertintinas kaip elgęsis

[5] 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.

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

itin aplaidžiai – nesuabejojęs, nepatikrinęs skambinusių asmenų ir jų nurodymų patikimumo ir galimo prieštaravimo tarp gautų nurodymų bei gautos SMS žinutės teksto, atskleidė vienkartinį saugos kodą tretiesiems asmenims ir šie veiksmai, taip pat mokėjimo kortelės duomenų atskleidimas, įgalino trečiuosius asmenis tiek susieti pareiškėjo mokėjimo kortelę su *Apple Pay* mokėjimo metodu, tiek ir įvykdyti mokėjimo operacijas.

Tai reiškia, kad mokėjimo operacijas tretieji asmenys be pareiškėjo žinios galėjo atlikti tik dėl to, kad pareiškėjas, būdamas labai neatsargus, netinkamai vykdė Mokėjimų įstatymo (34 straipsnis) ir privatiems klientams taikomose sąlygose įtvirtintus mokėjimo kortelės saugaus naudojimo reikalavimus. Taigi, labiausiai tikėtina, kad būtent pareiškėjas dėl didelio neatsargumo 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 priklausantį 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 mokėtojui 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 mokėjimo operacijų lėšų ir pareiškėjo reikalavimas, kad bankas grąžintų pareiškėjui mokėjimo operacijų lėšas, atmestinas kaip nepagrįstas.

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

Atmesti 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 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