LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

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

2022-10-24 Nr. 429-527
Vilnius

Lietuvos bankas gavo X. X. (toliau – pareiškėjas) kreipimąsi, kuriuo prašoma išnagrinėti tarp pareiškėjo ir *Revolut Bank UAB* (buvusi *Revolut Payments UAB*[1]) (toliau – bankas) kilusį ginčą.

N u s t a t y t a:

2020 m. gruodžio 4 d. pareiškėjas ir bankas sudarė mokėjimo paslaugų teikimo sutartį (toliau – Sutartis), kurios pagrindu pareiškėjui buvo atidaryta mokėjimo sąskaita Nr. (*duomenys neskelbiami*) (toliau – sąskaita) ir išduota su šia sąskaita susieta „MasterCard" mokėjimo kortelė Nr. (*duomenys neskelbiami*) (toliau – kortelė).

2022 m. birželio 1 d. 19 val. 1 min. kortelė buvo pridėta prie mobiliųjų mokėjimų sistemos „Apple Pay" (toliau – *Apple Pay* sistema) ir per šią sistemą 19 val. 16 min. kortele buvo inicijuota 2 000 EUR mokėjimo operacija (toliau – ginčijama mokėjimo operacija) kriptoturto keityklai „Mercuryo" (toliau – gavėja). Ginčijamos mokėjimo operacijos suma buvo iš karto rezervuota pareiškėjo sąskaitoje.

Tą pačią dieną, t. y. birželio 1 d., 19 val. 22 min. pareiškėjas kreipėsi į banką, informavo, kad iš jo apgaulės būdu buvo išvilioti kortelės duomenys ir panaudoti ginčijamai mokėjimo operacijai inicijuoti, ir prašė atšaukti šios mokėjimo operacijos vykdymą. Bendraudamas su banku, pareiškėjas paaiškino, kad per interneto svetainę *www.donedeal.ie* norėjo parduoti jam priklausantį daiktą, su juo susisiekė tariamas daikto pirkėjas, atsiuntė jam SMS žinutę su šia nuoroda *https://anpost.receive-pay.info/receive/90692212*, ją paspaudęs, pareiškėjas atsidariusiame lange suvedė savo kortelės duomenis, kad gautų iš tariamo pirkėjo lėšas už parduodamą daiktą, o iš karto po to pastebėjo, kad jo sąskaitoje buvo inicijuota ginčijama mokėjimo operacija. Pareiškėjas pabrėžė, kad neautorizavo ginčijamos mokėjimo operacijos ir jokių kodų tretiesiems asmenims neatskleidė. Bankas pranešė pareiškėjui, kad užblokavo jo kortelę, ir informavo, kad jei per 16 dienų nebus gautas gavėjos patvirtinimas apie galutinį atsiskaitymą, pareiškėjo sąskaitoje atlikta lėšų rezervacija bus panaikinta. Atsižvelgdamas į pareiškėjo patiriamus nepatogumus, bankas taip pat suteikė pareiškėjui galimybę du mėnesius nemokamai naudotis paslaugų planu „Premium".

2022 m. birželio 2 d. bankas informavo pareiškėją, kad netenkins pareiškėjo prašymo, nes nustatė, kad ginčijama mokėjimo operacija buvo inicijuota per *Apple Pay* sistemą, o pareiškėjas buvo pirmiau patvirtinęs bankui, kad pareiškėjo įrenginys yra jo žinioje. Bankas atkreipė pareiškėjo dėmesį į tai, kad kartu su inicijuotomis mokėjimo operacijomis pateikti gavėjo duomenys kartais gali nesutapti su tais duomenimis, kuriuos klientai mato įsigydami iš gavėjo prekės ar paslaugas, todėl klientams gali vėliau klaidingai atrodyti, kad jie neatpažįsta kažkurios mokėjimo operacijos.

Gavęs banko atsakymą pareiškėjas tą pačią dieną, t. y. 2022 m. birželio 2 d., informavo banką, kad nesutinka su banko atsakymu. Pareiškėjas paaiškino, kad naudoja „Samsung" išmanųjį telefoną, kuris nesudaro galimybės naudotis *Apple Pay* sistema, ir jokių kitų įrenginių, iš kurių būtų galima naudotis *Apple Pay* sistema, pareiškėjas neturi. Pareiškėjas pateikė bankui savo įrenginio ekrano nuotraukas, kuriose užfiksuotas pareiškėjo ir tariamo daikto pirkėjo susirašinėjimas, įskaitant tariamo pirkėjo pareiškėjui siųstą nuorodą. Pareiškėjas pabrėžė, kad turi įsigijęs vertybinių popierių ir kriptoturto, tačiau žino, kada ir kokius mokėjimus atlieka. Pareiškėjas

[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*.

teigė, kad nežino gavėjos ir jai ginčijamos mokėjimo operacijos neatliko. Tą pačią dieną bankas informavo pareiškėją, kad esant piniginių lėšų rezervacijai negali inicijuoti tarptautinės kortelių organizacijos „MasterCard" (toliau – *MasterCard* organizacija) lėšų grąžinimo procedūros ir kad būtina palaukti iki tol, kol paaiškės, ar per pirmiau nurodytą 16 dienų terminą gavėjas pateiks patvirtinimą dėl galutinio atsiskaitymo.

2022 m. birželio 3 d. bendrovė informavo pareiškėją, kad 2022 m. birželio 2 d. gavo iš gavėjo galutinį patvirtinimą dėl atsiskaitymo kortele ir nurašė iš pareiškėjo sąskaitos ginčijamos mokėjimo operacijos sumą. Bankas paaiškino pareiškėjui, kokia tvarka ir sąlygomis bankas turi vykdyti mokėjimo kortelėmis inicijuotas mokėjimo operacijas, ir nurodė, kad *MasterCard* organizacijos lėšų grąžinimo procedūra ginčijamos mokėjimo operacijos atžvilgiu yra negalima, nes ši mokėjimo operacija atlikta ir autorizuota bekontakčiu būdu per *Apple Pay* sistemą.

2022 m. birželio 9 d. pareiškėjas pakartotinai kreipėsi į banką, informavo, kad nesutinka su banko sprendimu negrąžinti jam ginčijamos mokėjimo operacijos sumos, pateikė bankui policijos įstaigai pateikto pareiškimo kopiją, dar kartą pakartotojo, kad neturi įrenginio, kuriuo galėtų naudotis *Apple Pay* sistema, ir papildomai nurodė, kad savo naudojamame įrenginyje nebuvo gavęs jokių autorizacijos piršto atspaudu pranešimų ir neautorizavo ginčijamos mokėjimo operacijos.

2022 m. birželio 20 d. bankas informavo pareiškėją, kad *MasterCard* organizacijos lėšų grąžinimo procedūra nebus inicijuota ir šis banko sprendimas yra galutinis ir nekeičiamas.

Nesutikdamas su banko sprendimu, pareiškėjas kreipėsi į Lietuvos banką dėl kilusio vartojimo ginčo nagrinėjimo. Pareiškėjas prašė Lietuvos banko rekomenduoti bankui grąžinti (kompensuoti) jam ginčijamos mokėjimo operacijos sumą. Pareiškėjo teigimu, ginčijama mokėjimo operacija buvo inicijuota apgaulės būdu, jis nebuvo gavęs jokių autorizacijos piršto atspaudu pranešimų ir šios mokėjimo operacijos neautorizavo. Pareiškėjas taip pat nurodė, kad neturi ir nėra turėjęs įrenginio, kuriame būtų galima naudotis *Apple Pay* sistema, ir niekada šia sistema nesinaudojo. Apie šias aplinkybes pareiškėjas teigė pranešęs iki nurašant ginčijamos mokėjimo operacijos sumą iš pareiškėjos sąskaitos, t. y. kai lėšos pareiškėjo sąskaitoje buvo dar tik rezervuotos, bet bankas vis tiek įvykdė ginčijamą mokėjimo operaciją ir nurašė jos sumą iš sąskaitos.

Atsiliepime į pareiškėjo kreipimąsi bankas nurodė nesutinkantis su pareiškėjo reikalavimu ir prašė jį atmesti. Banko teigimu, ginčijama mokėjimo operacija buvo atlikta ir autorizuota panaudojant bekontaktį mokėjimo (atsiskaitymo) metodą per *Apple Pay* sistemą. Bankas pabrėžė, kad banko klientai, įskaitant pareiškėją, turi teisę pridėti banko išduotas mokėjimo kortelės prie *Apple Pay* sistemos iš bet kurio įrenginio, kuriame yra galimybė naudotis *Apple Pay* sistema, ir toks įrenginys nebūtinai turi būti (neprivalo būti) susietas su įrenginiu, kuriame įdiegta „Revolut" programėlė, ir (arba) kurį klientas įprastai naudoja sutartinių santykių su banku metu. Bankas taip pat paaiškino, kad, norint pridėti mokėjimo kortelę prie *Apple Pay* sistemos, reikia ne tik šioje sistemoje nuskenuoti mokėjimo kortelę arba rankiniu būdu įvesti mokėjimo kortelės duomenis (numerį, galiojimo datą, kortelės saugos kodą CVV), bet ir, tai padarius, patvirtinti mokėjimo kortelės pridėjimą prie šios sistemos, įvedant banko SMS žinute į kliento telefono numerį, kurį klientas nurodo ir patvirtina bankui sudarant mokėjimo sutartį, siųstą vienkartinį saugos kodą, kuris galioja 30 min. nuo jo atsiuntimo. Banko vidaus sistemų duomenimis, pridedant pareiškėjo kortelę prie *Apple Pay* sistemos, buvo suvesti teisingi kortelės duomenys ir teisingas vienkartinis saugos kodas.

Bankas atkreipė dėmesį, kad pareiškėjas neneigė, kad, paspaudęs iš tariamo daikto pirkėjo gautą SMS žinutę su nuoroda, atsidariusiame lange atskleidė savo kortelės duomenis. Bankas pateikė įrodymus, patvirtinančius, kad SMS žinutė su vienkartiniu saugos kodu, skirtu patvirtinti kortelės pridėjimą prie *Apple Pay* sistemos, į pareiškėjo telefono Nr. (*duomenys neskelbiami*) (toliau – telefono numeris) buvo išsiųsta 2022 m. birželio 1 d. 19 val. Minėjote SMS žinutėje bankas taip pat įspėjo pareiškėją, kad šiuo vienkartiniu saugos kodu negalima dalintis su kitais asmenimis. Bankas pabrėžė, kad nesuvedus vienkartinio saugos kodo kortelės pridėjimas prie *Apple Pay* sistemos nebūtų buvęs patvirtintas ir atsiskaitymas per *Apple Pay* sistemą būtų neįmanomas, taip pat papildomai paaiškino, kad, jei vienkartinis saugos kodas būtų įvestas neteisingai, kortelės pridėjimo prie *Apple Pay* sistemos procesas būtų kartojamas iš naujo, t. y. vėl reikėtų nuskenuoti kortelę arba rankiniu būdu suvesti pirmiau nurodytus kortelės duomenis, gauti naują vienkartinį saugos kodą, o tada jį suvesti, taip patvirtinant kortelės pridėjimą prie *Apple Pay* sistemos.

Bankas neteigė, kad įrenginys, naudotas pridėti kortelę prie *Apple Pay* sistemos ir per šią sistemą inicijuoti ginčijamą mokėjimo operaciją, priklausė būtent pareiškėjui, tačiau pabrėžė, kad

be aktyvaus pareiškėjo dalyvavimo, t. y. kortelės duomenų ir vienkartinio saugos kodo atskleidimo, tretieji asmenys nebūtų galėję pridėti pareiškėjo kortelės prie *Apple Pay* sistemos ir vėliau per šią sistemą inicijuoti ginčijamos mokėjimo operacijos. Atsižvelgdamas į tai, bankas nurodė manantis, kad pareiškėjas atskleidė tretiesiems asmenims ne tik kortelės duomenis, bet ir suvedė vienkartinį saugos kodą ir (arba) atskleidė jį tretiesiems asmenims, kurie panaudojo šį kodą kortelės pridėjimui prie *Apple Pay* sistemos patvirtinti.

Komentuodamas atsisakymo inicijuoti *MasterCard* organizacijos lėšų grąžinimo procedūrą priežastis, bankas paaiškino, kad *MasterCard* organizacija nenustato galimybės ginčyti mokėjimo operacijos tuo pagrindu, kad ji buvo atlikta dėl sukčiavimo, kai mokėjimo kortelės turėtojas dalyvavo vykdant mokėjimo operaciją. Kadangi pareiškėjas autorizavo kortelės pridėjimą prie *Apple Pay* sistemos ir (arba) aktyviais savo veiksmais, t. y. pats patvirtino arba perdavė vienkartinį saugos kodą tretiesiems asmenims, kad šie patvirtintų kortelės pridėjimą prie *Apple Pay* sistemos, bankas teigė neturėjęs teisės inicijuoti *MasterCard* organizacijos lėšų grąžinimo procedūros.

Nors ir laiko ginčijamą mokėjimo operaciją tinkamai autorizuota paties pareiškėjo, bankas papildomai nurodė manantis, kad nagrinėjamoje situacijoje pareiškėjas, atskleisdamas tretiesiems asmenims kortelės duomenis ir vienkartiniu saugos kodu pats patvirtinęs kortelės pridėjimą prie *Apple Pay* sistemos ir (arba) perduodamas šį vienkartinį saugos kodą tretiesiems asmenims, taip sudarymas galimybę šiems asmenims patvirtinti kortelės pridėjimą prie *Apple Pay* sistemos, elgėsi itin neatsargiai ir nesilaikydamas Lietuvos Respublikos mokėjimų įstatymo 34 straipsnyje ir Sutarties 9 punkte pareiškėjui nustatytų pareigų, susijusių su kortelės ir jos duomenų naudojimu bei saugojimu.

Bankas papildomai atkreipė dėmesį, kad net ir bendrovės „AnPost" interneto svetainėje, į kurią, kaip teigė pareiškėjas, jis buvo nukreiptas per iš tariamo daikto pardavėjo SMS žinute gautą nuorodą, yra aiškiai ir didelėmis raidėmis įspėta saugotis sukčių, neteisėtai apsimetančių šia bendrove[2]. Banko teigimu, pareiškėjas, būdamas bent vidutiniškai apdairus ir rūpestingas, ypač pirmą kartą, kaip jis pats teigė, parduodamas daiktą, turėjo pasidomėti, kaip vyksta tokie ir panašūs pardavimo sandoriai, o ne teirautis tariamo daikto pirkėjo, ar jis turėtų spausti jo atsiųstą nuorodą[3], ir ją paspaudęs atskleisti savo kortelės ir (ar) kitus duomenis.

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 42^1 straipsnyje reglamentuotų patikrinimų, skirtų faktinėms aplinkybėms, susijusioms su Lietuvos banko priežiūrimo finansų rinkos dalyvio galimu Lietuvos banko kompetencijai priskirtų teisės aktų reikalavimų pažeidimu, nustatyti ir įvertinti. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą ir jo pagrindu priima sprendimą.

Pareiškėjo ir banko ginčas kilo dėl banko atsisakymo grąžinti (kompensuoti) pareiškėjui ginčijamos mokėjimo operacijos sumą (iš viso 2 000 EUR) pagrįstumo.

Pareiškėjas savo reikalavimą grąžinti (kompensuoti) ginčijamos mokėjimo operacijos sumą argumentavo tuo, kad ši mokėjimo operacija buvo įvykdyta be pareiškėjo sutikimo, trečiajam asmeniui apgaulės būdu išviliojus iš jo kortelės duomenis, kurie be jo žinios vėliau buvo panaudoti ginčijamai mokėjimai operacijai atlikti, tačiau bankas net ir po to, kai buvo informuotas apie šias aplinkybes, įvykdė ginčijamą mokėjimo operaciją. Bankas teigė, kad ginčijama mokėjimo operacija buvo autorizuota šalių sutartu būdu, atlikta per *Apple Pay* sistemą, prie kurios naudojantis tik pareiškėjui žinomu vienkartiniu saugos kodu buvo pridėta ir patvirtina pareiškėjo kortelė, todėl bankas neturi pareigos savo lėšomis kompensuoti pareiškėjui ginčijamos mokėjimo operacijos sumos. Dėl pirmiau įvardytų priežasčių bankas taip pat teigė neturėjęs teisės ginčijamų mokėjimo operacijų atžvilgiu inicijuoti *MasterCard* organizacijos lėšų grąžinimo procedūros.

Šalių ginčas kilo iš jas siejančių mokėjimo paslaugų teikimo santykių. Mokėjimo paslaugų

---

[2] Pranešimo originalia kalba tekstas: „Be scam aware. We are aware of fraudsters sending fake emails and texts to customers pretending from AnPost. Visit our security hub to find information and tips to avoid scams messages. "

[3] Bankas komentuoja pareiškėjo bankui pateiktoje susirašinėjimo su tariamu daiktų pirkėju kopijoje nurodytą informaciją, iš kurios matyti, kad po to, kai tariamas daikto pirkėjas atsiuntė pareiškėjui nuorodą ir paprašė patvirtinti mokėjimą, informuodamas, kad tariamai apmokėjo daikto pristatymo per kurjerį paslaugas, pareiškėjas informavo tariamą daikto pirkėją, kad pirmą karą tokiu būdu parduoda daiktą, ir teiravosi jo, ar turėtų spausti jo atsiųstą nuorodą.

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 Mokėjimų įstatymas.

Siekiant išspręsti tarp pareiškėjos ir banko kilusį ginčą, Lietuvos banko vertinimu, būtina nustatyti, ar: 1) ginčijamos mokėjimo operacijos laikytinos autorizuotomis; 2) bankas turėjo (turi) pareigą grąžinti (kompensuoti) pareiškėjui ginčijamos mokėjimo operacijos sumą; 3) bankas turėjo (turi) pareigą ginčijamos mokėjimo operacijos atžvilgiu inicijuoti *MasterCard* organizacijos lėšų grąžinimo procedūrą.

1. Dėl ginčijamų mokėjimo operacijų autorizavimo

Mokėjimų įstatymo 29 straipsnio 1 dalyje nustatyta, kad mokėjimo operacija laikoma autorizuota tik tada, kai mokėtojas duoda sutikimą ją vykdyti. Mokėtojas gali duoti sutikimą įvykdyti vieną arba kelias mokėjimo operacijas. Sutikimas gali būti duodamas ir per lėšų gavėją. Jei sutikimo nėra, laikoma, kad mokėjimo operacija yra neautorizuota (Mokėjimų įstatymo 29 straipsnio 2 dalis). Vadovaujantis Mokėjimų įstatymo 13 straipsnio 3 dalies 3 punktu ir 29 straipsnio 1 punktu, sutikimo davimo sąlygos ir tvarka turi būti aptartos mokėtojo ir jo mokėjimo paslaugų teikėjo sudaromoje mokėjimo paslaugų teikimo sutartyje.

Ginčo nagrinėjimo metu nustatyta, kad ginčijamos mokėjimo operacijos buvo atliktos per *Apple Pay* sistemą, prie kurios buvo pridėta pareiškėjo kortelė.

Bankas nurodė, kad kortelės pridėjimas prie *Apple Pay* sistemos buvo patvirtintas vienkartiniu saugos kodu, kurį bankas siuntė į telefono numerį. Byloje neturima duomenų, kam priklausė *Iphone* įrenginys, kuriuo kortelė buvo pridėta prie *Apple Pay* sistemos. Atsižvelgdamas į tai, kad pareiškėjas tvirtino neturintis ir nenaudojantis įrenginių, sudarančių galimybę naudotis *Apple Pay* sistema, ir į tai, kad savo atsiliepime bankas taip pat neteigė ir neįrodinėjo, kad *Iphone* įrenginys galėjo priklausyti pareiškėjui ir (arba) būti jo žinioje, Lietuvos bankas daro išvadą, kad *Iphone* įrenginys priklausė ir (arba) buvo valdomas trečiųjų asmenų.

Banko teigimu, šių veiksmų atlikimas, nepaisant to, kas faktiškai pridėjo kortelę prie *Apple Pay* sistemos (pats pareiškėjas ar trečiasis asmuo), remiantis Sutarties 14 punktu, laikomas pareiškėjo sutikimo vykdyti kortele per *Apple Pay* sistemą inicijuotas mokėjimo operacijas davimu. Minėtame Sutarties punkte nustatyta, kad: „Mokėjimus atlikti ir išgryninti pinigų taip pat galite naudodamiesi „Revolut" kortele. Tai galite padaryti įvesdami savo „Revolut" kortelės duomenis (kortelės numerį, galiojimo datą ir CVC numerį) arba PIN kodą. <…> Sutikimą atlikti mokėjimus savo „Revolut" kortele taip pat duodate: <…> pateikdami „Revolut" kortelės numerį ir kitą informaciją prekybininkui ar paslaugų teikėjui ir patvirtindami šį mokėjimą naudojant „3D Secure" metodą <…>" Remdamasis Sutarties 14 punktu ir vidaus sistemų duomenimis, kurie patvirtina, kad bankas 2022 m. birželio 1 d. 19 val. pareiškėjo telefono numeriu išsiuntė SMS žinutę su vienkartiniu saugos kodu, skirtu kortelės pridėjimui prie *Apple Pay* sistemos patvirtinti, netrukus po to kortelės pridėjimas prie šios sistemos buvo patvirtintas šiuo kodu ir ginčijama mokėjimo operacija buvo inicijuota per *Apple Pay* sistemą, bankas laiko ginčijamą mokėjimo operaciją autorizuota paties pareiškėjo.

Kaip matyti, darydamas pirmiau nurodytas išvadas, bankas iš esmės rėmėsi tik jo vidaus sistemose užfiksuotais įvykiais ir jų atitikmeniu Sutartyje bendrais bruožais apibrėžtiems sutikimo vykdyti mokėjimo operacijas davimo kriterijais, neatsižvelgdamas į pareiškėjo nurodytas kortelės duomenų atskleidimo tretiesiems asmenims aplinkybes ir atskirai nevertindamas ginčijamos mokėjimo operacijos inicijavimo aplinkybių (pvz., kaip ir kada ir gavėjas gavo kortelės duomenis ir (arba) sutikimą jų pagrindu inicijuoti ginčijamą mokėjimo operaciją), nors būtent šios aplinkybės, Lietuvos banko nuomone, turi esminės reikšmės, vertinant, ar ginčijama mokėjimo operacija laikytina autorizuota.

Mokėjimo operacijų autorizuotumo klausimai negali būti vertinami izoliuotai, t. y. vien tik remiantis faktu, kad mokėtojo veiksmai formaliai atitinka mokėtojo ir mokėjimo paslaugų teikėjo sutartus sutikimo vykdyti mokėjimo operacijas davimo kriterijus, ypač tada, kai turima duomenų, kad mokėtojas, nors ir atliko šiuos veiksmus, neturėjo tikslo atlikti jokių mokėjimo operacijų (lėšų pervedimų) ir (arba) galimai nesuprato, kad tokiais savo veiksmais sudaro galimybę tretiesiems asmenims inicijuoti mokėjimo operacijas. Vadovaujantis Mokėjimų įstatymo 37 straipsnio 3 dalimi, mokėtojo mokėjimo paslaugų teikėjo užregistruotas mokėjimo priemonės (nagrinėjamu atveju – kortelės) naudojimas nebūtinai yra pakankamas įrodymas, kad mokėtojas autorizavo mokėjimo operaciją. Taigi, vien aplinkybė, kad banko vidaus sistemose buvo užfiksuota, kad, atliekant ginčijamas mokėjimo operacijas, buvo panaudoti pareiškėjo kortelės duomenys ir (arba) kad

bankas buvo siuntęs pareiškėjui vienkartinį saugos kodą, kuris buvo panaudotas pridedant kortelę prie *Apple Pay* sistemos, savaime neįrodo, kad ginčijama mokėjimo operacija buvo atlikta esant pareiškėjo valiai ir sutikimui, kaip jis suprantamas Mokėjimų įstatymo 29 straipsnio 1 dalyje.

Pažymėtina, kad valia yra esminis kiekvieno sandorio, kaip teisinio veiksmo, kuriuo siekiama sukurti tam tikras teises ir pareigas, elementas[4]. Taigi, mokėtojo valia atlikti konkrečią mokėjimo operaciją taip pat yra viena iš esminių aplinkybių, į kurią turėtų būti atsižvelgta, vertinant, ar mokėjimo operacija, kurios autorizuotumą mokėtojas ginčija, laikytina autorizuota. Mokėtojo valios išraiškos forma turėtų būti vertinama, atsižvelgiant į ją atspindinčių ir pagrindžiančių ginčijamų mokėjimo operacijų inicijavimo ir vykdymo aplinkybių bei šias aplinkybes pagrindžiančių ir (arba) paneigiančių įrodymų visumą.

Remiantis pareiškėjo bankui nurodyta informacija, pareiškėjas gavo SMS žinutę su nuoroda iš, kaip jis manė, tariamo daikto pardavėjo ir, paspaudęs SMS žinutėje pateiktą nuorodą, atsidariusiame lange suvedė kortelės duomenis, turėdamas tikslą gauti lėšas už parduotą daiktą, tačiau po kurio laiko pamatė, kad buvo inicijuota ginčijama mokėjimo operaciją. Pareiškėjas pateikė bankui įrodymus, patvirtinančius minėtos SMS žinutės su nuoroda gavimą. Pareiškėjas ne kartą pabrėžė bankui, o vėliau Lietuvos bankui, kad neautorizavo ginčijamos mokėjimo operacijos, t. y. kad pareiškėjo valios ir sutikimo atlikti ginčijamą mokėjimo operaciją nebuvo. Bankas nepateikė jokių įrodymų, kurie paneigtų pareiškėjo nurodytas aplinkybes. Byloje nėra duomenų, kurie leistų teigti, kad pareiškėjas būtų siekęs įsigyti ir (arba) būtų įsigijęs iš gavėjos paslaugas ir (ar) prekes ir, siekdamas atsiskaityti už jas, galėjo būti perdavęs gavėjai savo kortelės duomenis, įskaitant sutikimą naudoti juos ginčijamai mokėjimo operacijai inicijuoti. Duomenų, kad po ginčijamos mokėjimo operacijos įvykdymo gavėja būtų suteikusi pareiškėjui kokias nors paslaugas ir (arba) prekes, taip pat nėra. Taigi, remiantis byloje turimais duomenimis, pagrindo teigti, kad pareiškėjas galėjo tiesiogiai kontaktuoti su gavėja, perduoti jai savo kortelės duomenis ir (arba) kitu būdu duoti jai sutikimą inicijuoti ginčijamą mokėjimo operaciją, Lietuvos bankas neturi. Priešingai, byloje turimi duomenys leidžia daryti išvadą, kad kortelės duomenys, kaip ir nurodė pareiškėjos atstovas, galėjo būti išvilioti iš pareiškėjo apgaulės būdu, siekiant juos panaudoti neteisėtais tikslais, t. y. pasisavinti lėšas iš pareiškėjo sąskaitos. Pirma, pareiškėjui buvo atsiųsta SMS žinutė su nuoroda, kurią siuntė ne gavėja, o tariamas daikto pirkėjas. Remiantis pareiškėjo bankui nurodyta informacija, suklaidintas tariamo daikto pirkėjo pareiškėjas manė, kad kortelės duomenis atskleidžia pašto paslaugų teikėjui „An Post" (toliau – tariamas kurjeris), kuris neva turėjo paimti iš pareiškėjo parduotą daiktą ir pristatyti jį tariamam daikto pirkėjui, taip pat perduoti pareiškėjui lėšas už parduotą daiktą. Byloje neturima duomenų, kad tariamas daikto pirkėjas ir (arba) tariamas kurjeris būtų prašęs pareiškėjo pridėti kortelę prie *Apple Pay* sistemos ir (arba) informavęs pareiškėją, kad jo kortelė turi būti pridėta prie šios sistemos. Antra, *iPhone* įrenginys, kuriuo kortelė buvo pridėta prie *Apple Pay* sistemos, kaip konstatuota pirmiau, nepriklausė pareiškėjui ir nebuvo jo žinioje. Atkreiptinas dėmesys, kad pats bankas patvirtino, kad *iPhone* įrenginys banko ir pareiškėjo sutartiniuose santykiuose iki tol nebuvo naudotas, ir neneigė, kad jis galėjo priklausyti tretiesiems asmenims, o ne pareiškėjui.

Pažymėtina ir tai, kad tiek Mokėjimų įstatymo 29 straipsnio 1 dalyje, tiek Sutarties 14 punkte aiškiai įvardyta, kad veiksmus, kurie pareiškėjo, kaip mokėtojo, ir banko, kaip mokėtojo mokėjimo paslaugų teikėjo, susitarimu reikš sutikimo vykdyti mokėjimo operacijas davimu, aktyviais veiksmais turi atlikti pats pareiškėjas. Kaip ir nurodyta pirmiau, bankas pateikė įrodymus, patvirtinančius, kad ginčijama mokėjimo operacija buvo inicijuota pagal pareiškėjo kortelės duomenis ir kad iki ginčijamos mokėjimo operacijos inicijavimo pareiškėjo kortelė buvo pridėta panaudojant vienkartinį saugos kodą, kuris buvo išsiųstas pareiškėjo telefono numeriu, tačiau įrodymų, kurie patvirtintų, kad vienkartinį saugos kodą pridėdamas kortelę prie *Apple Pay* sistemos panaudojo, kortelės duomenis gavėjai perdavė ir (arba) kitu būdu savo sutikimą inicijuoti ginčijamą mokėjimo operaciją gavėjai davė pats pareiškėjas, nepateikė. Lietuvos banko vertinimu, esant duomenų, kad mokėtojui išduota mokėjimo priemone ir (arba) jos duomenimis galėjo būti pasinaudota neteisėtai, t. y. tam, kad iš mokėtojo mokėjimo sąskaitos būtų atliktos mokėjimo operacijos, ir neturint objektyvių ir pakankamų įrodymų, kad šios mokėjimo operacijos atliktos esant mokėtojo valiai ir sutikimui, tokios mokėjimo operacijos negalėtų būti laikomis autorizuotomis.

Įvertinęs ginčo šalių pateiktus paaiškinimus ir įrodymus, Lietuvos bankas nenustatė

[4] „Apgaulės atveju sudarytas sandoris yra ne sandorio šalies laisvos valios išraiškos rezultatas, o kitos sandorio šalies ar trečiojo asmens nesąžiningų veiksmų rezultatas. Jeigu apgaulės nebūtų buvę, apgautoji sandorio šalis sandorio arba apskritai nebūtų sudariusi, arba būtų sudariusi jį visiškai kitokiomis sąlygomis." (Lietuvos Aukščiausiojo Teismo 2016 m. gegužės 12 d. nutartis civilinėje byloje Nr. 3K-3-268-421/2016).

objektyvių ir pakankamų pagrindų, leidžiančių teigti, kad ginčijama mokėjimo operacija buvo įvykdytos esant pareiškėjo valiai ir sutikimui, kaip jis suprantamas Mokėjimų įstatymo 29 straipsnio dalies kontekste, todėl laiko ginčijamą mokėjimo operaciją neautorizuota.

2. Dėl neautorizuotos ginčijamos mokėjimo operacijos pasekmių ir pareiškėjo teisės į šios mokėjimo operacijos sumos grąžinimą

Vadovaujantis Mokėjimų įstatymo 38 straipsnio 1 dalimi, nesant Mokėjimų įstatymo 39 straipsnio 1 ir 3 dalyje nustatytų aplinkybių, mokėtojo mokėjimo paslaugų teikėjas privalo grąžinti mokėtojui visą neautorizuotos mokėjimo operacijos sumą ne vėliau kaip iki 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). 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 to paties įstatymo 34 straipsnyje nustatytų pareigų, susijusių su mokėjimo priemonėmis ir personalizuotais saugumo duomenimis (Mokėjimų įstatymo 39 straipsnio 3 dalis). Mokėjimų įstatymo 34 straipsnis nustato mokėtojui, kuriam išduota mokėjimo priemonė, pareigą naudotis šia mokėjimo priemone pagal jos išdavimą ir naudojimą reglamentuojančias sąlygas, o sužinojus apie jos praradimą, vagystę arba neteisėtą pasisavinimą ar neautorizuotą jos naudojimą, nedelsiant apie tai pranešti mokėjimo paslaugų teikėjui arba jo nurodytam subjektui (Mokėjimų įstatymo 34 straipsnio 1 dalis), taip pat, gavus mokėjimo priemonę, imtis veiksmų, kad būtų apsaugoti personalizuoti saugumo duomenys (Mokėjimų įstatymo 34 straipsnio 2 dalis). Vadovaujantis Mokėjimų įstatymo 37 straipsnio 1 ir 3 dalimis, pareiga įrodyti, kad mokėjimo operacijos autentiškumas buvo patvirtintas, ji buvo tinkamai užregistruota, įrašyta į sąskaitas ir jos nepaveikė techniniai trikdžiai arba kiti mokėjimo paslaugų teikėjo teikiamos paslaugos trūkumai, tenka mokėtojo mokėjimo paslaugų teikėjui. Mokėjimų įstatymo 39 straipsnio 4 dalyje nustatyta, kad, kai mokėtojo mokėjimo paslaugų teikėjas nereikalauja saugesnio autentiškumo patvirtinimo, mokėtojui dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai tenka tik tuo atveju, jeigu jis veikė nesąžiningai.

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 tada, kai įrodomas mokėtojo sukčiavimas (nesąžiningumas arba tyčia) arba didelis neatsargumas (Mokėjimų įstatymo 37 straipsnio 3 dalis ir 39 straipsnio 3 dalis), ir (arba) tik tada, kai mokėtojo mokėjimo paslaugų teikėjas nereikalauja saugesnio autentiškumo patvirtinimo ir nenustatomas pareiškėjo nesąžiningumas (Mokėjimų įstatymo 39 straipsnio 4 dalis).

Byloje neturima duomenų, kad nagrinėjamu atveju pareiškėjas galėjo elgtis nesąžiningai ir (arba) tyčia, todėl galimas mokėtojo sukčiavimas, kaip pagrindas atleisti mokėtojo mokėjimo paslaugų teikėją nuo pareigos atlyginti mokėtojui nuostolius dėl neautorizuotos mokėjimo operacijos įvykdymo, šiame sprendime atskirai nebus plačiau analizuojamas.

Byloje turimi duomenys leidžia daryti išvadą, kad nagrinėjamu atveju bankas taikė saugesnio autentiškumo patvirtinimo reikalavimus, t. y. reikalavo, kad kortelės prie *Apple Pay* sistemos pridėjimas būtų patvirtintas vienkartiniu saugos kodu, kuris išsiųstas pareiškėjo telefono numeriu ir turėjo likti žinomas tik pačiam pareiškėjui, nesuvedus kodo kortelės pridėjimas prie *Apple Pay* sistemos nebūtų buvęs įmanomas, todėl saugesnio autentiškumo patvirtinimo reikalavimų netaikymas, kaip pagrindas taikyti mokėtojo mokėjimo paslaugų teikėjui atsakomybę už nuostolius, atsiradusius dėl neautorizuotos mokėjimo operacijos įvykdymo, šiame sprendime taip pat atskirai nebus plačiau analizuojamas.

Kaip minėta pirmiau, bankas savo sprendimą negrąžinti (nekompensuoti) pareiškėjui ginčijamos mokėjimo operacijos sumos grindžia aplinkybe, kad ginčijama mokėjimo operacija buvo tinkamai autorizuota, t. y. pareiškėjo kortelę, kuria ši mokėjimo operacija buvo atlikta, prie *Apple Pay* sistemos pridėjus taikant saugesnio autentiškumo patvirtinimo procedūrą, tačiau kartu nurodo, kad pareiškėjo elgesiui būdingas ir didelis neatsargumas. Tai reiškia, kad, atsižvelgiant į pirmiau minėtas Mokėjimų įstatymo nuostatas, taip pat ir į šiuos banko teiginius, siekiant įvertinti, ar bankas pagrįstai atsisako grąžinti (kompensuoti) pareiškėjui ginčijamos mokėjimo operacijos, kurią Lietuvos bankas, priešingai, nei teigė bankas, vis dėlto laiko neautorizuota, sumą ir ar pareiškėjui galėtų būti taikoma Mokėjimų įstatymo 39 straipsnio 3 dalis, būtina nustatyti, ar pareiškėjo elgesys, atskleidžiant kortelės duomenis ir (ar) atliekant kitus veiksmus, dėl kurių galėjo būti įvykdyta ginčijama mokėjimo operacija, vertintini kaip didelis neatsargumas, dėl kurio visi nuostoliai, atsiradę dėl ginčijamos mokėjimo operacijos įvykdymo, turėtų tekti pačiam

pareiškėjui.

Mokėtojo neatsargumo laipsnio vertinimas yra susijęs su ginčo byloje nustatytų individualių, specifinių aplinkybių, kurias patvirtina ginčo byloje esantys įrodymai ir (arba) yra šalių neginčijamos neautorizuotos mokėjimo operacijos įvykdymo aplinkybės, visumos vertinimu. Taigi, išvada dėl mokėtojo paprasto ar didelio neatsargumo, kaip vertinamojo pobūdžio aplinkybė, negali būti daroma izoliuotai, išsamiai neįvertinus viso neautorizuotos mokėjimo operacijos įvykdymo ir su juo susijusių aplinkybių konteksto.

Kriterijai, į kuriuos reikėtų atsižvelgti vertinant kaltės laipsnį, yra iš dalies suformuluoti Antrosios mokėjimo paslaugų direktyvos preambulės 72 punkte: „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 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" (Lietuvos Aukščiausiojo Teismo 2017 m. balandžio 13 d. nutartis civilinėje byloje Nr. e3K-3-180-378/2017, 29 punktas).

Byloje neturima duomenų, kad nagrinėjamam ginčui aktualiu laikotarpiu į banko vidaus sistemas būtų įsilaužta ir (arba) jas būtų paveikę techniniai trikdžiai, dėl kurių pareiškėjo kortelės duomenys ir (arba) pareiškėjai siųstas vienkartinis saugos kodas galėjo tapti žinomas tretiesiems asmenims ir (arba) dėl kurių tretieji asmenys dėl nuo banko priklausančių aplinkybių būtų kitaip įgiję galimybę neteisėtai pasinaudoti pareiškėjo kortele, jos ir (arba) su jos naudojimu susijusiais duomenimis ir (arba) sąskaita. Vadinasi, pirmiau minėti duomenys tretiesiems asmenims turėjo tapti žinomi kitu būdu.

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 Sutarties 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 Sutarties nuostatos aiškiai nustato, kad už mokėjimo priemonės ir 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 reglamentuojančias sąlygas, jei būtų nustatyta, kad jis ėmėsi adekvačių veiksmų (arba nuo tam tikrų veiksmų susilaikė), kad būtų tinkamai užtikrintas kortelės ir kitų su jos naudojimu susijusių duomenų, sudarančių sąlygas inicijuoti ir tvirtinti mokėjimus, konfidencialumas.

Pareiškėjas pripažino, kad pats atskleidė savo kortelės duomenis, t. y. suvedė juos paspaudęs į telefono numerį gautoje SMS žinutėje pateiktą nuorodą, tačiau neigė gavęs pranešimus, prašančius atlikti autorizaciją piršto atspaudu, tai atlikęs ir (arba) atskleidęs jam siųstus ir (arba) kitaip žinomus kodus. Bankas pateikė įrodymus, patvirtinančius, kad SMS žinutė su vienkartiniu saugos kodu buvo išsiųsta pareiškėjo telefono numeriu. Pareiškėjo telefono numeris, kuriuo bankas jam siuntė pirmiau nurodytą SMS žinutę, sutampa su telefono numeriu, kurį pareiškėjas nurodė Lietuvos bankui, kreipdamasis dėl tarp šalių kilusio vartojimo ginčo nagrinėjimo. Taigi, pagrindo teigti, kad pareiškėjas galėjo negauti banko siųstos SMS žinutės, nėra. Esant tokiai situacijai, kai byloje turimų duomenų visuma leidžia daryti išvadą, kad pareiškėjas galimai atliko veiksmus, dėl kurių prarado ir (ar) tretiesiems asmenims atskleidė duomenis, kurie turėjo būti žinomi tik jam, bet pareiškėjas neigia atlikęs tokius veiksmus, įvertinti konkrečių pareiškėjo, kaip mokėtojo, veiksmų atsargumo laipsnį yra neįmanoma arba įmanoma apie jo veiksmus darant tik labiausiai tikėtinas prielaidas. Įrodymų pakankamumo taisyklė civiliniame procese grindžiama vadinamąja tikėtinumo taisykle (tikimybių pusiausvyros principu). 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]. Įvertinus tai, kad, nepatvirtinus kortelės pridėjimo prie *Apple Pay* sistemos vienkartiniu saugos kodu, kortelės pridėjimas prie šios sistemos nebūtų buvęs įmanomas, darytina išvada, kad nagrinėjamu atveju labiausiai tikėtina, kad, priešingai, nei teigė pareiškėjas, jis vis dėlto atskleidė tretiesiems asmenims šį kodą.

Pareiškėjas nurodė, kad, atskleisdamas kortelės duomenis, nesiekė atlikti jokių mokėjimų ir šiuos duomenis atskleidė kitais tikslais, t. y. siekdamas gauti lėšas už parduotą daiktą. Iš byloje turimų duomenų matyti, kad iki ginčijamos mokėjimo operacijos įvykdymo banko išduota mokėjimo kortele (-ėmis) pareiškėjas naudojasi nuo 2020 m. gruodžio mėnesio, o iki tol, t. y. nuo 2019 m. balandžio mėn., naudojosi analogiškomis *Revolut Ltd* paslaugomis. Taigi, pareiškėjo turima naudojimosi mokėjimo kortelėmis patirtis, Lietuvos banko vertinimu, turėjo būti pakankama, kad jis galėtų (turėtų) suprasti, kad kortelės duomenų, SMS žinute gauto vienkartinio saugos kodo atskleidimas ar kitokio autorizavimo veiksmo atlikimas yra sietini su lėšų iš sąskaitos, su kuria susieta kortelė, pervedimu, o ne gavimu, o pirmiau nurodytų veiksmų atlikimas, neturint tikslo kortele atlikti jokių mokėjimų, gali lemti tam tikras teisines pasekmes, t. y. kortelės duomenų praradimą, neteisėtą jų panaudojimą ir (ar) neautorizuotų mokėjimo operacijų iš sąskaitos, su kuria susieta kortelė, įvykdymą.

Vertinant tą faktą, kad pareiškėjas, kaip konstatuota pirmiau, atskleidė savo kortelės duomenis ir vienkartinį saugos kodą, gavęs iš nepažįstamo jam asmens, t. y. tariamo daikto pirkėjo, SMS žinutę su nuoroda, manytina, kad nagrinėjamu atveju pareiškėjo pasitikėjimas šiuo asmeniu ir (arba) jo teikiama informacija laikytinas visiškai nepagrįstu. Kaip matyti iš bylos duomenų, pareiškėjui nekėlė įtarimų nei tai, kodėl jo prašoma atskleisti savo kortelės duomenis, jei jis yra daikto pardavėjas, o ne pirkėjas, ir (ar) kodėl, jei šie duomenys reikalingi, kaip manė pareiškėjas, kurjeriui, SMS žinutę su nuoroda pareiškėjui siuntė tariamas pirkėjas, o ne tariamas kurjeris, nei tai, kodėl tariamas pirkėjas negalėjo atsiskaityti su pareiškėju tiesiogiai, pervesdamas lėšas į jo nurodytą sąskaitą, ir pan.

Iš viešai prieinamos informacijos matyti, kad tikrojo pašto paslaugų teikėjo „AnPost", veikiančio Airijos Respublikoje, kurioje gyvena ir pats pareiškėjas, oficiali interneto svetainė yra *https://www.anpost.com/*, nors tariamo daikto pirkėjo pareiškėjui siųstoje nuorodoje nurodytas interneto svetainės adresas buvo *https://anpost.receive-pay.info/receive/90692212*. Pastebėta, kad įprastai sukčiavimo atvejais sukčių suklastotos interneto svetainės vizualiai atrodo labai panašios į tikrąsias žinomų paslaugų teikėjų interneto svetaines, todėl vartotojui, kuris neturi specialių žinių, gali atrodyti, kad veiksmus su savo mokėjimo priemone jis atlieka tikroje žinomo paslaugų teikėjo interneto svetainėje. Kadangi tariamo daikto pirkėjo pareiškėjui SMS žinute siųstoje nuorodoje buvo minimas tikrojo pašto paslaugų teikėjo „AnPost" pavadinimas, manytina, kad pareiškėjas, prieš tai viešoje erdvėje nepatikrinęs tikrojo paslaugų interneto svetainės adreso, galėjo nepastebėti suklastotos ir tikrosios interneto svetainių skirtumų ir galvoti, kad yra nukreipiamas į tikrojo paslaugų teikėjo interneto svetainę, kurioje turi pateikti savo kortelės duomenis, kad, kaip jis tuo metu manė, gautų lėšas už parduodamą daiktą. Vis dėlto svarbu pažymėti, kad tikrasis pašto paslaugų teikėjas „AnPost" savo interneto svetainėje *https://www.anpost.com/Security* viešai įspėja apie galimus sukčiavimus, kurie pasireiškia neteisėtu šio paslaugų teikėjo pavadinimo naudojimu ir elektroninių laiškų ar žinučių siuntimu, taip pat atkreipia dėmesį, kad šis paslaugų teikėjas nei telefonu, nei elektroniniu paštu ar kitomis žinutėmis neprašo atskleisti mokėjimo sąskaitų, mokėjimo kortelių, PIN kodų ar kitokių slaptažodžių, taip pat nesiunčia jokių nuorodų. Lietuvos banko nuomone, pareiškėjas turėjo kritiškai vertinti gautos SMS žinutės ir paskesniuose žingsniuose rodomos informacijos turinį, suprasti, kad jo prašoma atlikti veiksmus, kurie nebūdingi norint gauti lėšas iš kito fizinio asmens, ir susilaikyti nuo bet kokių tolesnių veiksmų, kol nepasitikrino, kodėl jo prašoma atlikti šiuos veiksmus, ir neįsitikino, ar toks prašymas yra pagrįstas ir teisėtas.

Net jei pareiškėjas tuo metu nepagalvojo, kad kortelės duomenų atskleidimas gali sukelti jam neigiamų pasekmių, tolesni jo veiksmai (nereagavimas į banko jam teikiamą informaciją ir vienkartinio saugos kodo atskleidimas), kurių pareiškėjas taip pat kritiškai tuo metu nevertino, Lietuvos banko nuomone, rodo pareiškėją buvus itin neatsargų. Pažymėtina, kad banko pareiškėjui atsiųstoje SMS žinutėje su vienkartiniu saugos kodu buvo pakankamai aiškiai nurodyta, kad šis saugos kodas yra susijęs su *Apple Pay* sistemos naudojimu. Jei, kaip jis teigė, pareiškėjas neturėjo įrenginio, kuriame būtų galima naudotis *Apple Pay* sistema, gavus minėtą

[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.*

SMS žinutę iš banko, jam iš karto turėjo kilti įtarimas, kodėl jam siunčiama tokia SMS žinutė ir kažkoks kodas, jei jis *Apple Pay* sistema nesinaudojo ir nesiekė naudotis. Byloje neturima duomenų, kad, gavęs iš banko minėtą SMS žinutę, pareiškėjas būtų kreipęsis į banką ir mėginęs išsiaiškinti tokios žinutės siuntimo priežastis. Pažymėtina ir tai, kad šioje SMS žinutėje bankas buvo aiškiai nurodęs, kad vienkartinio saugos kodo negalima atskleisti tretiesiems asmenims, tačiau, kaip konstatuota pirmiau, pareiškėjas, pažeisdamas SMS žinutėje nurodytą draudimą, vis dėlto atskleidė vienkartinį saugos kodą tretiesiems asmenims ir taip sudarė jiems galimybę pridėti kortelę prie *Apple Pay* sistemos ir vėliau per ją inicijuoti ginčijamą mokėjimo operaciją.

Įvertinus ginčo byloje turimus duomenis, darytina išvada, kad nagrinėjamu atveju pareiškėjas jam išduota kortele ir su ja susijusiais duomenimis, įskaitant vienkartinį saugos kodą, naudojosi nesilaikydamas kortelės išdavimą ir naudojimą reglamentuojančių sąlygų ir nevykdė Mokėjimų įstatymo 34 straipsnyje 1 dalies 1 punkte ir 2 dalyje bei Sutarties 9 punkte jam nustatytų pareigų.

Mokėjimų įstatymo 39 straipsnio 5 dalyje nustatyta, kad mokėtojas neturi patirti jokių nuostolių dėl prarastos, pavogtos ar neteisėtai pasisavintos mokėjimo priemonės po to, kai pateikia šio įstatymo 34 straipsnio 1 dalies 2 punkte nurodytą pranešimą, išskyrus atvejus, kai jis veikė nesąžiningai. Vertinant, ar mokėtojo mokėjimo paslaugų teikėjui, remiantis Mokėjimų įstatymo 39 straipsnio 5 dalies nuostatomis, gali tekti pareiga atlyginti mokėtojui nuostolius, patirtus dėl neautorizuotos mokėjimo operacijos įvykdymo, Lietuvos banko nuomone, būtina atsižvelgti ne tik į Mokėjimų įstatymo 34 straipsnio 1 dalies 2 punkte nurodyto pranešimo apie neautorizuotos mokėjimo operacijos įvykdymą faktą, bet ir į šio pranešimo pateikimo laiką ir aplinkybes, kurios jau buvo faktiškai įvykusios, kai šis pranešimas buvo pateiktas.

Bylos duomenimis, kad prarado kortelės duomenis ir jie buvo panaudoti neautorizuotoms ginčijamoms mokėjimo operacijoms atlikti, pareiškėjas informavo banką po to, kai bankas buvo gavęs mokėjimo nurodymą vykdyti ginčijamą mokėjimo operaciją ir jo pagrindu pareiškėjo sąskaitoje rezervavęs šios mokėjimo operacijos sumą. Duomenų, kurie leistų teigti, kad bankas, priimdamas vykdyti mokėjimo nurodymą atlikti ginčijamą mokėjimo operaciją, galėjo pažeisti Mokėjimų įstatymą, kitus jam taikomus teisės aktus ir (arba) *MasterCard* organizacijos taisykles, neturima. Objektyvaus pagrindo teigti, kad iki pareiškėjo kreipimosi į banką bankas galėjo (turėjo) suprasti, kad pareiškėjas galimai tapo sukčių auka ir ginčijama mokėjimo operacija yra inicijuota be pareiškėjo sutikimo ar žinios, taip pat nėra. Iš bylos duomenų matyti, kad pastarosios aplinkybės bankui tapo žinomos tik po to, kai, bankui priėmus vykdyti mokėjimo nurodymą ir rezervavus lėšas pareiškėjo sąskaitoje, pareiškėjas pats jį apie tai informavo. Vėlesnis šių aplinkybių paaiškėjimas nekeičia fakto, kad pareiškėjas, nors ir nesiekė ginčijamos mokėjimo operacijos įvykdymo, atliko tam tikrus veiksmus, kuriuos šalys iš anksto buvo sutarusios įprastomis sąlygomis laikyti pareiškėjo sutikimu vykdyti kortele inicijuotas mokėjimo operacijas. Pagal Lietuvos Respublikos civilinio kodekso 6.206 straipsnį, viena šalis negali remtis kitos šalies neįvykdymu tiek, kiek sutartis neįvykdyta dėl jos pačios veiksmų ar neveikimo arba kitokio įvykio, kurio rizika jai pačiai ir tenka. Taigi, panaudojęs kortelę ir jos duomenis kitais, negu mokėjimo operacijai iš savo sąskaitos inicijuoti, tikslais bei atskleidęs tretiesiems asmenims vienkartinį saugos kodą, skirtą kortelės pridėjimui prie *Apple Pay* sistemos patvirtinti, Lietuvos banko nuomone, pareiškėjas negalėtų remtis tuo, kad bankas, nežinodamas pirmiau nurodytos aplinkybės, neatsisakė vykdyti jam pateikto mokėjimo nurodymo atlikti ginčijamą mokėjimo operaciją ir jį šalių iš anksto sutarta tvarka ir sąlygomis priėmė vykdyti, nes būtent pareiškėjas pirmasis pažeidė šalių sutartas kortelės ir jos duomenų naudojimo ir saugojimo sąlygas, taip sudarydamas galimybę tretiesiems asmenims tariamai pareiškėjo vardu pateikti bankui šį mokėjimo nurodymą.

Mokėjimų įstatymo 29 straipsnio 3 dalyje nustatyta, kad mokėtojas bet kuriuo metu iki šio įstatymo 44 straipsnyje nustatyto neatšaukiamumo momento gali panaikinti sutikimą įvykdyti mokėjimo operaciją ir (arba) kelias mokėjimo operacijas. Vadovaujantis Mokėjimų įstatymo 44 straipsnio 1 dalimi, mokėjimo paslaugų vartotojas negali atšaukti mokėjimo nurodymo po to, kai jį gauna mokėtojo mokėjimo paslaugų teikėjas, išskyrus šiame straipsnyje nustatytas išimtis. Mokėjimų įstatymo 44 straipsnio 2 dalyje nustatyta, kad kai mokėjimo operacija inicijuojama gavėjo arba per gavėją, mokėtojas negali atšaukti mokėjimo nurodymo po to, kai gavėjui davė sutikimą atlikti mokėjimo operaciją. Kaip matyti, Mokėjimų įstatymo 44 straipsnio 2 dalis nustato ankstesnį, negu to paties straipsnio 1 dalyje nurodytas, mokėjimo nurodymo neatšaukiamumo momentą. Kaip nurodyta pirmiau, tuo metu, kai pareiškėjas pranešė bankui apie ginčijamą mokėjimo operaciją, bankas jau buvo gavęs mokėjimo nurodymą vykdyti ginčijamą mokėjimo operaciją, t. y. pareiškėjas pateikė bankui Mokėjimų įstatymo 34 straipsnio 1 dalies 2 punkte

nurodytą pranešimą po to, kai suėjo Mokėjimų įstatymo 44 straipsnio 1 dalyje ir 2 dalyje nustatyti terminai, per kuriuos mokėtojas turi teisę atšaukti mokėjimo nurodymą. Suėjus šiems terminams, mokėjimo nurodymas gali būti atšauktas tik tada, kai dėl to susitaria mokėjimo paslaugų vartotojas ir atitinkamas mokėjimo paslaugų teikėjas ir yra gaunamas gavėjo sutikimas (Mokėjimų įstatymo 44 straipsnio 4 dalis).

Ginčo byloje nustatytos faktinės aplinkybės, šalių pateikti paaiškinimai ir įrodymai leidžia daryti išvadą, kad pareiškėjas galėjo iš anksto, t. y. iki bankas gavo mokėjimo nurodymą vykdyti ginčijamą mokėjimo operaciją ir jo pagrindu rezervavo lėšas pareiškėjo sąskaitoje, pastebėti galimą kortelės duomenų praradimą, neautorizuotą jų naudojimą ir (arba) ketinimą juos naudoti. Kadangi pareiškėjas dėl galimo kortelės duomenų praradimo į banką kreipėsi po to, kai šių duomenų pagrindu buvo atlikta ginčijama mokėjimo operacija ir bankui buvo pateiktas mokėjimo nurodymas jas vykdyti, o bankas, nesant gavėjo sutikimo, nebegalėjo jo atšaukti, darytina išvada, kad nėra pagrindo pareiškėjo atžvilgiu taikyti Mokėjimo įstatymo 39 straipsnio 5 dalies nuostatas.

Byloje nėra duomenų, kad gavėjas būtų davęs sutikimą atšaukti ginčijamos mokėjimo operacijos vykdymą, priešingai – iš bylos duomenų matyti, kad kitą dieną po mokėjimo nurodymo bankui pateikimo, gavėjas (per savo finansų įstaigą) pateikė bankui galutinį patvirtinimą dėl atsiskaitymo kortele, kurio pagrindu bankas nurašė lėšas iš pareiškėjo sąskaitos. Taigi, Mokėjimų įstatymo 44 straipsnio 4 dalyje nurodyta sąlyga (gavėjo sutikimas atšaukti mokėjimo nurodymus) nebuvo tenkinta, todėl ginčijamos mokėjimo operacijos atšaukimas nebuvo galimas.

Įvertinęs pirmiau nurodytas aplinkybes, šalių pateiktus įrodymus ir jų pagrindu padarytas išvadas, Lietuvos bankas mano, kad pareiškėjo elgesys, kuris pasireiškė tuo, kad pareiškėjas, gavęs iš nepažįstamos asmens SMS žinutę su nuoroda ir ją atsidaręs, neturėdama tikslo kortele atlikti lėšų pervedimo operacijų, atsidariusiame lange (-uose) atskleidė savo kortelės duomenis, taip sudarydamas sąlygas tretiesiems asmenims inicijuoti kortelės prie *Apple Pay* sistemos pridėjimą, atskleidė tretiesiems asmenims banko jam siųstą vienkartinį saugos kodą, kuriuo buvo patvirtintas kortelės pridėjimas prie *Apple Pay* sistemos, ir taip sudarė tretiesiems asmenims galimybę, panaudojant kortelės duomenis, per šią sistemą inicijuoti ginčijamą mokėjimo operaciją iš jo sąskaitos, pripažintinas kaip elgesys, iš esmės besiskiriantis nuo atsargaus elgesio reikalavimų, t. y. laikytinas itin neatsargiu, kuris galiausiai lėmė, kad pareiškėjo sąskaitoje buvo įvykdytos neautorizuotos ginčijamos mokėjimo operacijos. Byloje turimi duomenys leidžia teigti, kad jeigu nagrinėjamu atveju pareiškėjas būtų buvęs pakankamai atidus ir kritiškas jam teiktos, anksčiau jau turėtos ir (arba) žinomos informacijos bei savo atliekamų veiksmų atžvilgiu, jis būtų pastebėjęs ir supratęs, kad atlieka veiksmus, kurių, ne tik kad nereikia atlikti, bet ir, laikantis Mokėjimų įstatymo 34 straipsnyje ir Sutarties 9 punkte pareiškėjui nustatytų pareigų, negalima atlikti, ir ginčijama mokėjimo operacija galimai nebūtų įvykdyta. Atsižvelgiant į tai, konstatuotina, kad nagrinėjamu atveju yra pagrindas pareiškėjui taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį.

3. Dėl MasterCard organizacijos lėšų grąžinimo procedūros inicijavimo

Bankas nurodė, kad vertino galimybę inicijuoti *MasterCard* organizacijos lėšų grąžinimo procedūrą, tačiau nustatė, kad ginčijamos mokėjimo operacijos atžvilgiu ji yra negalima.

Vertinant banko atsisakymo inicijuoti *MasterCard* organizacijos lėšų grąžinimo procedūrą pagrįstumą, svarbu pažymėti, kad nei Lietuvos Respublikos teisės aktai, nei tiesioginio taikymo Europos Sąjungos teisės aktai nereglamentuoja, kokiomis konkrečiomis sąlygomis turi būti vykdoma *MasterCard* organizacijos lėšų grąžinimo procedūra. Taigi, banko veiksmus, susijusius su *MasterCard* organizacijos prekės ženklo kortelėmis atliktų mokėjimo operacijų užginčijimu, reglamentuoja *MasterCard* organizacijos taisyklės, kurios nustato atvejus ir tvarką, pagal kurią bankas, gavęs *MasterCard* mokėjimo kortelės turėtojo prašymą, turi teisę kreiptis į *MasterCard* organizaciją dėl lėšų grąžinimo procedūros inicijavimo.

Įvertinus *MasterCard* organizacijos taisyklių[6] 92 puslapyje nurodytas sąlygas, nustatančias mokėjimo operacijų ginčijimą tuo pagrindu, kad jos buvo įvykdytos sukčiavimo būdu, matyti, kad, kaip ir buvo nurodęs bankas, *MasterCard* organizacija nesuteikia bankui teisės inicijuoti lėšų grąžinimo procedūros pirmiau nurodytu pagrindu, kai mokėjimo kortelės turėtojas dalyvauja vykdant mokėjimo operaciją, t. y. kai mokėjimo operacijos buvo tinkamai patvirtintos ir identifikuotos, įskaitant vėlesnes operacijas, susijusias su pradine patvirtinta mokėjimo operacija, ir tapatybės patikrinimą ir skaitmeninius saugius nuotolinius mokėjimus[7]. Taigi, pagrindo teigti,

[6] https://www.mastercard.us/content/dam/public/mastercardcom/na/global-site/documents/chargeback-guide.pdf

[7] Cituojama nuostata originalo kalba: „This section provides information in handling a dispute when the cardholder states that the cardholder did not engage in the transaction. A No Cardholder Authorization chargeback must not be processed for any of the following: <…> Properly authenticated and identified transactions (including any subsequent transaction related to the original authenticated transaction, such as a

kad bankas nepagrįstai atsisakė inicijuoti *MasterCard* lėšų grąžinimo procedūrą, nėra.

Konstatavus, kad nagrinėjamu atveju yra pagrindas pareiškėjo atžvilgiu taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, nustatančią, kad mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai, ir nenustačius kitų aplinkybių, dėl kurių bankui kiltų (galėtų kilti) pareiga grąžinti pareiškėjui ginčijamos mokėjimo operacijos sumą, pareiškėjos reikalavimas rekomenduoti bankui grąžinti (kompensuoti) pareiškėjui ginčijamos mokėjimo operacijos sumą yra 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 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

partial shipment or recurring payment) in authorization (DE 48, subelement 42 [Electronic Commerce Indicators], subfield, 1 (Electronic Commerce Security Level Indicator and UCAF Collection Indicator), positions 1, 2, and 3) with the values of 211, 212, 215, 217, 221, 222, 225, 241, 242, or 245. Examples include, but are not limited to, Identity Check and Digital Secure Remote Payment (DSRP).”