



**LIETUVOS BANKO
PRIEŽIŪROS TARNYBOS
TEISĖS IR LICENCIJAVIMO DEPARTAMENTO
DIREKTORIUS**

**SPRENDIMAS
DĖL X.X. IR AB SEB BANKO GINČO NAGRINĖJIMO**

2021-05-13 Nr. 429-165
Vilnius

Lietuvos bankas gavo pareiškėjo X.X. (toliau – pareiškėjas) kreipimąsi, kuriuo prašoma išnagrinėti tarp pareiškėjo ir AB SEB banko (toliau – bankas) kilusį ginčą.

Nustatyta:

2021 m. sausio 15 d. 16:38 val. pareiškėjas per *Viber* programėlę gavo asmens, prisistačiusio pirkėju, (toliau – pirkėjas) žinutę, kurioje teiraujamas, ar pareiškėjas dar parduoda prekę (svarstyklės), ir pateikta nuoroda į *skelbiu.lt* puslapyje esantį pareiškėjo skelbimą apie parduodamą prekę. Pirkėjas pareiškėjui per *Viber* programėlę atsiuntė žinutę su nuoroda ir paprašė nuorodą paspausti ir patvirtinti pirkėjo pinigų perlaidą pareiškėjui (atsiskaitymą už prekę). Paspaudęs pirkėjo atsiųstą nuorodą pareiškėjas pateko į interneto svetainę, kurioje buvo pateikta informacija apie tai, kad asmuo, kurio vardas ir pavardė nesutapo su pirkėjo vardu ir pavarde, į pareiškėjo banko sąskaitą ketina pervesti 15 Eur. Atidaręs pirkėjo atsiųstą nuorodą pareiškėjas pamatė, kad jo prašoma suvesti asmens duomenis (vardą ir pavardę) bei mokėjimo kortelės duomenis (kortelės numerį, galiojimo datą, CVC kodą). Kai atidarytoje nuorodoje buvo suvesti asmens bei mokėjimo kortelės duomenys, pareiškėjas buvo nukreiptas į kitą interneto langą, kuriame buvo prašoma įvesti savo banko sąskaitos likutį bei patvirtinti asmens tapatybę suvedant banko atpažinimo kodą bei SmartID PIN1. Kai suvedė banko atpažinimo kodą ir SmartID PIN1, pareiškėjui kilo įtarimų, todėl jis prisijungė prie savo interneto banko paskyros banke. Minėtoje paskyroje pareiškėjas pastebėjo, kad iš jo banko sąskaitos buvo nurašyti 204 Eur gavėjai *duomenys neskelbiami* (mokėjimas atliktas per pervedimą tarpininką WALLETABU_INT_IN\100). Pareiškėjas 2021 m. sausio 15 d. 19:27 val. telefonu kreipėsi į banką, pranešė apie jo neautorizuotą mokėjimo operaciją ir paprašė ją atšaukti bei gražinti pareiškėjui 204 Eur.

2021 m. sausio 18 d. bankas pareiškėją informavo, kad neturi galimybės mokėjimo operacijos užginčyti tarptautinės mokėjimo kortelių organizacijos „MasterCard“ taisyklių nustatyta tvarka, nes ginčijama mokėjimo operacija buvo patvirtinta saugesniu autentifikavimo būdu (*3D secure*).

Pareiškėjas nesutiko su banko atsakymu ir kreipėsi į Lietuvos banką dėl vartojimo ginčo nagrinėjimo. Kreipimesi pareiškėjas paaiškino pirmiau minėtas ginčijamos mokėjimo operacijos atlikimo aplinkybes. Taip pat pareiškėjas teigė, kad pardavimais internetu neužsiima, todėl nežino visų galimų su tuo susijusių rizikų, o tuo metu, kai pirkėjo atsiųstoje nuorodoje vedė mokėjimo kortelės duomenis ir patvirtino savo tapatybę suveddamas banko atpažinimo kodą bei SmartID PIN1, buvo užsiėmęs kitais darbais, todėl jo budrumas buvo sumažėjęs. Pareiškėjas teigė, kad paprašytas suvesti banko atpažinimo kodą ir SmartID PIN1 neprisiminė prisijungimo prie SmartID kodo, todėl telefonu kreipėsi į SmartID klientų aptarnavimo padalinį. Pareiškėjas teigia, kad SmartID klientų aptarnavimo padalinio konsultantas įspėjo pareiškėją, kad jis galėjo susidurti su sukčiais, tačiau pareiškėjas vis tiek suvedė tiek banko atpažinimo kodą, tiek SmartID PIN1 kodą.

Pareiškėjas teigė nesuprantantis, kaip, jam suvedus SmartID PIN1, sukčiai galėjo užbaigti mokėjimo operaciją panaudodami *3D secure* kodą. Pareiškėjas teigia, kad bankas, turėdamas informaciją apie sukčiavimo atvejus, turėjo atšaukti ginčijamą mokėjimo operaciją arba jos nevykdyti. Pareiškėjas teigia, kad į banką dėl ginčijamos mokėjimo operacijos atšaukimo kreipėsi iš karto po to, kai tik pamatė, kad iš jo banko sąskaitos nurašyti pinigai,

tačiau bankas ginčijamos mokėjimo operacijos neatšaukė ir negražino ginčijamos mokėjimo operacijos lėšų.

Pareiškėjo nuomone, bankas nepakankamai įsigilino į situaciją, atliko skubotus veiksmus, todėl pareiškėjas Lietuvos banko prašė tarpininkauti gražinant ginčijamos mokėjimo operacijos lėšas ir imtis veiksmų, kad lėšų gavėjas gražintų pinigus.

Bankas pateiktame atsiliepime Lietuvos bankui paaiškino, kad ginčijama mokėjimo operacija buvo atlikta panaudojant mokėjimo kortelės duomenis (kortelės numerį, galiojimo datą, CVC kodą), o mokėjimo kortele inicijuotą mokėjimo operaciją pareiškėjas papildomai patvirtino interneto banke suveddamas banko atpažinimo kodą bei SmartID PIN1. Taigi bankas ginčijamą mokėjimo operaciją įvykdė tinkamai.

Bankas atkreipė dėmesį, kad toks mokėjimo operacijos panaudojant mokėjimo kortelę patvirtinimo būdas yra aptartas banko Bendrųjų taisyklių (toliau – Taisyklės) 2-ame priede, kurio 11 skyriuje nustatyta, kad „mokėtojas duoda sutikimą mokėti mokėjimo kortele, jei pateikia mokėjimo kortelės ir / ar savo duomenis prekybininkui ar paslaugos teikėjui ir, patvirtindamas mokėjimo operaciją, suveda savo interneto banko prisijungimo duomenis“. Banko teigimu, toks sutikimo įvykdyti mokėjimo operaciją davimo būdas laikomas saugesniu autentiškumo patvirtinimu ir laikomas tinkamai autorizuotu, t. y. atliktu paties pareiškėjo, todėl atsakomybė už tokį mokėjimą tenka pačiam pareiškėjui.

Pasisakydamas dėl ginčijamos mokėjimo operacijos atšaukimo, bankas paaiškino, kad tada, kai mokėtojas patvirtina mokėjimo operaciją, ji jau būna įvykdyta ir bankas jos atšaukti negali. Bankas paaiškino, kad, vadovaudamasis „MasterCard“ kortelių asociacijos taisyklėmis, negalėjo pradėti mokėjimo operacijos ginčijimo procedūros, nes mokėjimas buvo atliktas pervedimų tarpininkui (*Walletatabu_int_in*), kuris pareiškėjo prašymu pinigų pervedė galutiniam gavėjui. Bankas pažymėjo, kad lėšų pervedimo tarpininkai nėra prekės pardavėjai, todėl bankas neturi teisės pradėti mokėjimo operacijos ginčo procedūros „MasterCard“ organizacijoje.

2021 m. balandžio 19 d. bankas pateikė papildomus paaiškinimus dėl pareiškėjo pateikto reikalavimo bankui pagrįstumo. Bankas dar kartą pažymėjo, kad su pareiškėju susitarė dėl sutikimo įvykdyti mokėjimo operaciją panaudojant kortelę davimo formos ir tvarkos. Banko teigimu, ginčijama mokėjimo operacija kortele buvo inicijuota tokia tvarka, kaip nurodyta Taisyklėse – buvo panaudoti tik pareiškėjui žinomi duomenys: kortelės numeris, galiojimo laikas, CVC kodas, pareiškėjo vardas ir pavardė, suvesti pareiškėjo interneto banko prisijungimo duomenys – interneto banko naudotojo atpažinimo kodas ir pareiškėjo naudojamos atpažinimo priemonės SmartID PIN1 kodas, kurį į savo mobilųjį įrenginį gavo pareiškėjas.

Banko teigimu, atsižvelgiant į tai, kad buvo atlikti visi pareiškėjo ir banko sutarti mokėjimo operacijai kortele inicijuoti būtini veiksmai, galima teigti, kad pareiškėjas davė sutikimą įvykdyti mokėjimo operaciją, todėl nėra pagrindo teigti, kad ginčijama mokėjimo operacija yra neautorizuota, kaip nurodyta Lietuvos Respublikos mokėjimų įstatymo (toliau – Mokėjimų įstatymas) 29 straipsnio 2 dalyje (jeigu mokėtojo sutikimo įvykdyti mokėjimo operaciją nėra, laikoma, kad mokėjimo operacija yra neautorizuota).

Remdamasis Mokėjimų įstatymo 34 straipsnio 4 dalimi, kurioje nurodoma, kad tais atvejais „kai mokėtojo mokėjimo paslaugų teikėjas nereikalauja saugesnio autentiškumo patvirtinimo, mokėtoju dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai tenka tik tuo atveju, jeigu jis veikė nesažiningai“, bankas teigia, kad tada, kai mokėtojo mokėjimo paslaugų teikėjas reikalauja saugesnio autentiškumo patvirtinimo, nuostoliai, atsiradę dėl neautorizuotų mokėjimo operacijų, tenka mokėtoju.

Bankas pabrėžė, kad laikėsi Mokėjimų įstatymo 58 straipsnio 1 dalies 2 punkto reikalavimo mokėjimo paslaugų teikėjui taikyti saugesnio autentiškumo patvirtinimo procedūrą, kai mokėtojas inicijuoja elektroninę mokėjimo operaciją, ir Mokėjimų įstatymo 58 straipsnio 2 dalyje nustatyto papildomo reikalavimo, kai inicijuojama nuotolinė mokėjimo operacija, taikyti saugesnio autentiškumo patvirtinimo procedūrą, užtikrinančią dinamišką kiekvienos mokėjimo operacijos susiejimą su konkrečia suma ir konkrečiu gavėju.

Bankas patikino, kad, kaip mokėjimo paslaugų teikėjas, laiku ir tinkamai vykdė visus jam teisės aktų keliamus reikalavimus: „reikalavo, kad pareiškėjui atpažinti ir mokėjimo operacijai patvirtinti, būtų atlikti veiksmai, atitinkantys griežto kliento autentiškumo patvirtinimo reikalavimus, o saugesnio autentiškumo patvirtinimo procedūra, užtikrina dinamišką pareiškėjo inicijuotos mokėjimo operacijos susiejimą su mokėjimo operacijos suma ir konkrečiu gavėju“.

Pasisakydamas dėl ginčijamos mokėjimo operacijos autorizavimo vertinimo, bankas teigia, kad, nors Mokėjimų įstatyme tam, kad mokėjimo operacija būtų laikoma autorizuota, reikalaujama mokėtojo sutikimo mokėjimo operacijai įvykdyti, banko nuomone, mokėtojo sutikimas įvykdyti mokėjimo operaciją negali būti aiškinamas per plačiai. Bankas teigia, kad Mokėjimų įstatymas leidžia mokėtojui ir jo mokėjimo paslaugų teikėjui susitarti dėl sutikimo įvykdyti mokėjimo operaciją davimo formos, tai ir buvo aiškiai su pareiškėju susitarta sutartyje ir jos sudėtinėje dalyje Taisyklėse. „Sutikimo faktui konstatuoti neturi būti remiamasi vien tik pareiškėjo subjektyviaja puse, tačiau visų pirma, vertinami konkretūs pareiškėjo atlikti veiksmai bei kaip jie atitinka „formos“ kriterijų. Šio ginčo atveju, nėra jokių abejonių dėl formos bei dėl to, kad visus veiksmus – mokėjimo nurodymui suformavimui ir vykdymui būtinos informacijos pateikimą bei papildomo saugos sumetimais prašomo kodo atskleidimo veiksmus atliko pats pareiškėjas, kaip teigia, suklaidintas sukčių, todėl laikytina, jog pareiškėjo sutikimas vykdyti mokėjimo operaciją yra duotas, net jei pareiškėjas teigia to aiškiai nesupratęs, tačiau iš visos aplinkybių analizės matyti, jog toks nesupratimas nepanaikino sutikimui būtinų elementų buvimo.“

Bankas teigia, kad, įvertinus visas ginčo aplinkybes, matyti, kad pareiškėjas turėjo ir galėjo suprasti, kad inicijuoja lėšų pervedimo mokėjimo operaciją, o ne lėšų gavimo mokėjimo operaciją, „kadangi tokie elementai, kaip kortelės duomenys, papildomas saugos kodas ir autentifikavimosi procedūra, panaudojant prisijungimo duomenis, yra veiksmų seka bei būtini elementai, būtent mokėjimo operacijai atlikti (dėl šių būtinų elementų yra susitarta ir sutartyje su pareiškėju)“. Banko nuomone, suveddamas mokėjimo kortelės duomenis, banko atpažinimo kodą bei SmartID PIN1, pareiškėjas veikė itin neapdairiai, nesilaikė Mokėjimų įstatymo 34 straipsnyje nustatytų mokėjimo paslaugų vartotojo pareigų (naudotis mokėjimo priemone pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas bei gavus mokėjimo priemonę imtis veiksmų, kad būtų apsaugoti personalizuoti saugumo duomenys) ir naudojosi mokėjimo priemone ne pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas – kortelės duomenis, interneto banko atpažinimo kodą ir SmartID PIN1 kodą atskleidė tretiesiems asmenims.

Banko teigimu, pareiškėjo neatsargumą tretiesiems asmenims atskleidžiant kortelės duomenis, interneto banko atpažinimo kodą ir SmartID PIN1 kodą rodo šios ginčo byloje nustatytos aplinkybės: 1) pareiškėjas teigia, jog bendraudamas su potencialia pirkėja buvo „užsiėmęs kitais reikalais, todėl budrumas buvo sumažėjęs“. Banko vertinimu, toks pareiškėjo elgesys lėmė, kad veddamas kortelės duomenis pareiškėjas nebuvo atidus ir dėjo nepakankamas pastangas susipažinti, kur veda kortelės duomenis, kam pateikia banko atpažinimo kodus ir kokioje aplinkoje tai daro; 2) pareiškėjas kreipimesi dėl vartojimo ginčo nagrinėjimo nurodė, kad susirašinėjimas su sukčiais užsitęsė. Banko teigimu, ši aplinkybė leidžia daryti išvadą, kad pareiškėjas turėjo pakankamai laiko įvertinti savo veiksmus, vykdomos mokėjimo operacijos paskirtį ir detales bei nutraukti neatsargius veiksmus ir nevykdyti tolimesnių sukčių nurodymų; 3) pareiškėjas patvirtino, kad susirašinėjant su sukčiais jam kilo įtarimų, nes buvo prašoma suvesti savo banko sąskaitos likutį, banko atpažinimo kodą bei SmartID prisijungimo duomenis, tačiau jis į tai nekreipė tinkamo dėmesio, ypač vertinant tai, kad parduodant daiktą jis turėjo būti lėšų gavėjas, o ne mokėtojas, kuris turi patvirtinti mokėjimo operaciją; 4) pareiškėjas skambino į SmartID klientų pagalbos tarnybą ir jos darbuotojas įspėjo, kad atliekami veiksmai yra panašūs į sukčiavimo atvejus, tačiau pareiškėjas ir toliau vykdė sukčių nurodymus, nors, jo teigimu, jam buvo kilusių įtarimų; 5) pareiškėjas niekaip nesureagavo į pirkėjo teiginį apie *3D secure* patvirtinimo būtinumą kortelės operacijai. Bankas paaiškino, kad, vadovaujantis Taisyklių nuostatomis, „3D apsauga – papildomas kliento autentifikavimo būdas, kai kortelės turėtojas atlieka mokėjimo operaciją kortele elektroninėje parduotuvėje. Papildomas kliento autentifikavimas reikalauja kliento mokėjimo operaciją patvirtinti prisijungimu prie asmeninės internetinės bankininkystės paskyros, tuo tarpu pareiškėjas mokėjimą siekė ne įvykdyti, o gauti lėšas ir tai jam nesukėlė jokių įtarimų“; 6) „pareiškėjas identifikavo ir suprato, kad, nuspaudęs *Viber* programėle atsiųstą nuorodą, pateko į interneto puslapį, kurio adresą sukėlė įtarimą, tačiau papildomai netikrino, kad vis dar yra tame pačiame www.skelbiu.lt interneto puslapyje“.

Banko nuomone, visi pirmiau paminėti pareiškėjo veiksmai, kuriais jis inicijavo ir patvirtino ginčijamą mokėjimo operaciją siekdamas gauti lėšų, o ne jas pervesti, apdairiam ir patyrusiam paslaugų vartotojui, koks ir yra pareiškėjas, turėjo sukelti didelių įtarimų ir pareiškėjas galėjo suprasti savo atliekamų veiksmų reikšmę ir pasekmes. Bankas teigia, kad pareiškėjas yra patyręs mokėjimo paslaugų vartotojas, nes, banko turimais duomenimis, visus

veiksmus atliko ne pirmą kartą – „SmartID programėle naudojasi beveik 4 metus ir jau turėjo tokio pobūdžio mokėjimo operacijų (inicijuojamų panaudojant mokėjimo kortelę) atlikimo patirties, todėl jam turėjo būti žinoma tai, kad suvedus kortelės duomenis nuo su kortele susietos mokėjimo sąskaitos bus nurašytos lėšos“. Banko turimais duomenimis, pareiškėjas, panaudodamas tos pačios kortelės duomenis, anksčiau yra užsisakęs tokių paslaugų teikėjų kaip *Google, Netflix, Sony, Citybee* paslaugų.

Apibendrinamas savo papildomuose paaiškinimuose pateiktus argumentus, bankas pažymėjo, kad pareiškėjas tretiesiems asmenims atskleidė SmartID PIN1 kodą, interneto banko atpažinimo kodą ir kortelės duomenis, o pareiškėjo ginčijama mokėjimo operacija buvo įvykdyta pareiškėjo, kaip mokėtojo, tapatybę tinkamai patvirtinus jo turima priemone – SmartID. Banko teigimu, atsiliepime nurodytos aplinkybės pagrindžia pareiškėjo didelį neatsargumą. „Pareiškėjas dėl savo kaltės, pasireiškusios dideliu neatsargumu, sudarė sąlygas mokėjimo operacijos inicijavimui su trečiųjų asmenų įsikišimu, atskleidė personalizuotus saugos duomenis, kurie turėtų nuo tokio pobūdžio veikų klientus apsaugoti, nes nesilaikė elementarių saugumo reikalavimų, kurie suponuoja tai, jog vidutiniškai apdairus ir rūpestingas bei analogišką mokėjimo paslaugų vartojimo patirtį turintis asmuo analogiškoje situacijoje galėjo ir turėjo suvokti bei atpažinti, jog iš jo prašomų duomenų visuma būdinga duomenų, reikalingų mokėjimo operacijai inicijuoti, visumai, dėl ko pareiškėjas, be kita ko, yra aiškiai susitaręs sutartyje su banku.“

Papildomai bankas atkreipė dėmesį, kad nors ir laikosi pozicijos, kad ginčijama mokėjimo operacija yra autorizuota, nes dėl sutikimo davimo formos su pareiškėju buvo aiškiai susitarta ir dėl to abejonių nėra, Mokėjimų įstatymo 39 straipsnio 3 dalyje yra nustatytas ir visiškos atsakomybės už dėl didelio neatsargumo patirtus nuostolius principas.

Atsižvelgdamas į pirmiau nurodytų aplinkybių visumą, bankas teigia, kad neprivalo pareiškėjui kompensuoti dėl jo ginčijamos mokėjimo operacijos patirtų nuostolių.

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 banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjui 2021 m. sausio 18 d. pareiškėjo banko sąskaitoje atliktos 204 Eur mokėjimo operacijos (toliau – ginčijama mokėjimo operacija) sumą. Pareiškėjas teigia nedavęs sutikimo įvykdyti ginčijamą mokėjimo operaciją, todėl bankas turi grąžinti pareiškėjui šios operacijos sumą. Bankas teigia, kad pareiškėjas savo sutikimą ją įvykdyti davė pareiškėjo ir banko sudarytoje sutartyje sutarta tvarka – suveddamas savo asmens duomenis, mokėjimo kortelės duomenis ir savo tapatybę patvirtindamas suvedant banko atpažinimo kodą bei SmartID PIN1, todėl bankas neprivalo grąžinti pareiškėjui ginčijamos mokėjimo operacijos sumos. Siekiant išspręsti pareiškėjo ir banko ginčą, Lietuvos banko vertinimu, būtina nustatyti šias pagrindines aplinkybes: 1) ar ginčijama mokėjimo operacija laikytina autorizuota, t. y. ar šiai operacijai atlikti buvo gautas pareiškėjo sutikimas; 2) ar bankas turėjo (turi) pareigą grąžinti pareiškėjui ginčijamos mokėjimo operacijos 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 Mokėjimų įstatymas (redakcija, galiojusi nuo 2020 m. spalio 1 d.).

Dėl ginčijamos mokėjimo operacijos 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).

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).

Banko teigimu, pareiškėjo sutikimas įvykdyti ginčijamą mokėjimo operaciją kortele buvo duotas vienu iš pareiškėjo ir banko sudarytoje bendrojoje sutartyje nurodytų būdų – prekybininkui buvo pateikta mokėjimo kortelė, įskaitant ir CVC kodą, ir asmens duomenys ir mokėjimo operacija buvo patvirtinta suvedant banko atpažinimo kodą ir SmartID PIN1 kodą (3D secure).

Įvertinus pareiškėjo ir banko sudarytos bendrosios sutarties nuostatas, nustatyta, kad bendraja sutartimi bankas ir pareiškėjas buvo susitarę, kad asmens duomenų ir (arba) mokėjimo kortelės duomenų, įskaitant ir CVC kodą, suvedimas prekybininko puslapyje bei asmens tapatybės patvirtinimas suvedant banko atpažinimo kodą ir SmartID PIN1 laikoma pareiškėjo sutikimo atlikti mokėjimo operaciją davimu (*Taisyklių 2 priedo 11 skyrius „mokėtojas duoda sutikimą mokėti mokėjimo kortele, jei: pateikia mokėjimo kortelės ir / ar savo duomenis prekybininkui ar paslaugos teikėjui ir patvirtina mokėjimo operaciją 3D būdu; atsiskaito elektroninės prekybos ar paslaugų vietose ir įveda mokėjimo kortelės duomenis: mokėjimo kortelės numerį, galiojimo laiką, CVC kodą“*).

Atkreiptinas dėmesys į tai, kad Taisyklių 2 priedo 11 skyriuje kalbama apie atvejus, kai mokėtojas duoda savo sutikimą pervesti lėšas mokėjimo kortele prekybininkui arba paslaugų teikėjui, su kuriuo mokėtojas nori atsiskaityti, ir tuo tikslu perduoda mokėjimo kortelės ir kitus šioje Taisyklių nuostatoje nurodytus duomenis, vis dėlto nagrinėjamo ginčo atveju, priešingai nei nurodyta minimoje Taisyklių nuostatoje, pareiškėjas šiuos duomenis atskleidė ne todėl, kad ketino mokėjimo kortele pervesti lėšas, o norėdamas gauti pinigus už parduodamą prekę, t. y. šiuo konkrečiu atveju veikė kaip prekės pardavėjas, o ne kaip mokėtojas.

Pažymėtina ir tai, kad bankas, darydamas išvadą, kad ginčijama mokėjimo operacija buvo autorizuota Taisyklėse nustatyta tvarka paties pareiškėjo, iš esmės remiasi tik tuo faktu, kad mokėjimo operacijai įvykdyti buvo panaudoti mokėjimo kortelės duomenys ir suvestas banko atpažinimo kodas bei SmartID PIN1, tačiau nevertina, kada ir (arba) kas perdavė lėšų gavėjui ir (arba) jo mokėjimo paslaugų teikėjui duomenis, kurių pagrindu buvo inicijuota ginčijama mokėjimo operacijai, t. y. ar šiuos duomenis tiesiogiai pateikė pats pareiškėjas, ar iš pareiškėjo šiuos duomenis neteisėtai išvilioję asmenys.

Bankas pateikė jo vidaus sistemose užfiksuotus duomenis, pagrindžiančius, kad ginčijamos mokėjimo operacijos inicijavimo dieną 19:14:37 val. kartu su lėšų gavėjo nurodymu nurašyti lėšas iš pareiškėjo mokėjimo sąskaitos buvo pateikti pareiškėjo kortelės duomenys, reikalingi ginčijamai mokėjimo operacijai inicijuoti; 19:14:47 val. buvo nurodyta mokėjimo operacijos suma ir valiuta (204 Eur); 19:15:17 val. sėkmingai atlikta pareiškėjo autentifikacija jungiantis prie interneto banko, tačiau šie duomenys, Lietuvos banko vertinimu, dar neįrodo, kad visi šie veiksmai yra atlikti gavus pareiškėjo sutikimą. Atkreiptinas dėmesys į tai, kad vien aplinkybė, jog mokėtojo mokėjimo paslaugų teikėjo vidaus sistemose užregistruotas mokėtojui išduotos mokėjimo priemonės, įskaitant jos personalizuotus saugumo duomenis, naudojimas, nelaikytina pakankamu įrodymu, kad mokėjimo priemone naudojosi ir (arba) mokėjimo operaciją autorizavo pats mokėtojas (Mokėjimų įstatymo 37 straipsnio 3 dalis).

Lietuvos bankas paprašė banko papildomai pateikti informaciją apie banko vidaus sistemose užfiksuotus įrenginių, kuriais šiam ginčui nagrinėti aktuali laikotarpiu buvo jungtasi nuotoliniu būdu prie pareiškėjo interneto banko paskyros, IP adresus. Bankas pateikė banko vidaus sistemos išrašus, kuriuose pateikti duomenys apie laikotarpiu nuo 2020 m. gruodžio 1 d. iki 2021 m. sausio 15 d. banko sistemose fiksuotus IP adresus, kuriais buvo jungtasi prie pareiškėjo interneto banko paskyros (toliau – IP adresų sąrašas). Bankas atkreipė dėmesį, kad visus kartus jungtasi su SmartID bei užfiksuotas pareiškėjo mobilaus telefono numeris, nurodytas banko kontaktuose.

Iš Banko pateikto IP adresų sąrašo duomenų matyti, kad minimu laikotarpiu prie interneto banko buvo jungtasi iš šių IP adresų:

1) 2020 m. gruodžio 1 d. prie interneto banko sistemos buvo jungtasi iš IP adresu Nr. *duomenys neskelbiami* (toliau – IP adresas Nr. 1);

2) 2021 m. sausio 5 d. prie interneto banko sistemos buvo jungtasi iš IP adresu Nr. *duomenys neskelbiami* (toliau – IP adresas Nr. 2);

3) ginčijamos mokėjimo operacijos atlikimo dieną, t. y. 2021 m. sausio 15 d., 19:15:02 val. buvo jungtasi iš IP adresu Nr. *duomenys neskelbiami* (toliau – IP adresas Nr. 3).

Pateikdamas minėtą informaciją, bankas papildomai atkreipė dėmesį, kad „IP adresas

keičiasi naudojant skirtingas interneto prieigos vietas ir skirtingus įrenginius, pvz. jungiantis iš mobiliojo telefono IP adresus bus kitoks nei jungiantis iš kompiuterio ir pan. Dėl šios priežasties IP adresų gretinimas su konkrečiu kompiuteriu, mobiliuoju įrenginiu ar tarpusavyje (tarp IP adresų) yra nepatikimas.“

Siekdamas įvertinti, kurie iš banko nurodytų IP adresų priklauso pareiškėjui, Lietuvos bankas paprašė pareiškėjo nurodyti įrenginių, kuriais pareiškėjas jungėsi nagrinėjamu laikotarpiu, IP adresus. Pareiškėjas nurodė, kad mokėjimo kortelės duomenis, įskaitant CVC kodą bei asmens tapatybės patvirtinimą panaudojant SmartID PIN1, suvedė telefonu iš IP adreso *duomenys neskelbiami* (toliau – IP adresas Nr. 4), o jo kompiuterio IP adresus sutampa su banko nurodytu IP adresu Nr. 1.

Lietuvos bankas taip pat paprašė pareiškėjo nurodyti, kokią informaciją ir duomenis pareiškėjas matė, kai pirkėjo jam atsiųstoje nuorofoje, tikėdamasis, kad tvirtina 15 Eur lėšų gavimo į savo banko sąskaitą pervedimo operaciją, vedė savo asmens duomenis (vardą, pavardę) ir mokėjimo kortelės duomenis (kortelės numerį, galiojimo datą, CVC kodą) bei patvirtino tokią lėšų gavimo operaciją SmartID PIN1. Pareiškėjas nurodė, kad atkreipė dėmesį į tai, kad nuorofoje nurodyti pirkėjo duomenys nesutapo su asmens, su kuriuo jis bendravo dėl pareiškėjui priklausančios prekės pardavimo (šio asmens vardo ir pavardės pareiškėjas teigia neprisimenantis), tačiau, remiantis pareiškėjo pateikta informacija, jis šių duomenų nesutapimo tuo metu nesureiškė, nes tikėjo, kad tvirtina lėšų gavimo operaciją. Pareiškėjo teigimu, jį apgavusių asmenų pateiktoje nuorofoje jo buvo prašoma suvesti savo banko sąskaitoje tuo metu buvusį piniginių lėšų likutį, todėl į prašomą lauką jis suvedė 204 Eur, nesuprasdamas, kad jį apgavę asmenys šios informacijos prašo norėdami inicijuoti būtent šios sumos nurašymo iš jo banko sąskaitos operaciją. Iš duomenų, kurie pareiškėjui buvo rodomi pirkėju apsimitusio asmens pateiktoje nuorofoje, kad duoda sutikimą nurašyti lėšas iš jo banko sąskaitos, pareiškėjas teigia nesupratęs.

Papildomai pateiktuose paaiškinimuose dėl informacijos, kurią ginčui aktualiu laikotarpiu galėjo matyti pareiškėjas, bankas pažymėjo, kad „informacijos, kuri patvirtintų, kokius konkrečius vaizdus galimai matė pareiškėjas neturime, kadangi pareiškėjas, nuspaudus *Viber* programėlėje gautą nuorodą, buvo nukreiptas į kitą (galimai sukčių kontroliuojamą) interneto puslapį, kuriame ir atliko savo tolesnius veiksmus.“ Minėtas banko paaiškinimas leidžia pagrįstai daryti išvadą, kad bankas neneigia to fakto, jog pareiškėjas ginčijamai mokėjimo operacijai atlikti ir patvirtinti reikalingus duomenis galėjo suvesti trečiųjų asmenų kontroliuojamoje aplinkoje, kurioje pareiškėjui, kaip jis pats teigia, buvo rodoma tikrovės neatitinkanti informacija apie lėšų gavimo inicijuojamą mokėjimo operaciją, t. y. kad pareiškėjui galėjo būti rodoma informacija apie tai, kad jis tvirtina lėšų pervedimo į jo banko sąskaitą operaciją, o ne lėšų nurašymo iš jo banko sąskaitos operaciją. Lietuvos bankas neturi galimybės patikrinti, kokią su mokėjimo pavidimu susijusią informaciją trečiųjų asmenų pateiktoje interneto svetainėje matė pareiškėjas, tačiau pareiškėjo bei banko pateikta informacija, Lietuvos banko vertinimu, leidžia daryti išvadą, kad šio ginčo atveju yra didesnė tikimybė, kad trečiųjų asmenų aplinkoje, į kurią pareiškėjas pateko atidaręs pirkėju apsimitusio trečiojo asmens atsiųstą nuorodą, pareiškėjui apie pagal mokėjimo kortelės duomenis inicijuojamą mokėjimo operaciją buvo rodoma tikrovės neatitinkanti informacija, kuri galėjo suklaidinti pareiškėją dėl tokios mokėjimo operacijos esmės ir pobūdžio, taigi, pareiškėjas pagrįstai tikėdamasis, kad tvirtina lėšų gavimo mokėjimo operaciją, galėjo nesuprasti, kad šiuo konkrečiu atveju atlieka veiksmus, kurie banko ir pareiškėjo sutartiniuose santykiuose galėtų būti laikytini sutikimu atlikti mokėjimo operaciją iš kliento banko sąskaitos.

Lietuvos banko nuomone, nagrinėjant šį konkretų ginčą svarbu įvertinti ir tai, kad pareiškėjas SmartID PIN1 kodu tvirtindamas ginčijamą mokėjimo operaciją, kurią manė esant lėšų pervedimo į jo banko sąskaitą operaciją, galėjo suprasti, kad tvirtina lėšų pervedimo iš jo banko sąskaitos operaciją. Banko cituojamų Taisyklių 2 priedo 11 punkte, kuriuo bankas remiasi teigdamas, kad ginčijama mokėjimo operacija laikytina autorizuota paties pareiškėjo, nėra įvardyta, kurio SmartID PIN kodo (PIN1 ar PIN2) suvedimas banko ir pareiškėjo santykiuose yra laikytinas sutikimu, kad mokėjimo operacija būtų atlikta. Tokia informacija detalizuota banko interneto svetainėje adresu <https://www.seb.lt/privatiems/el-bankininkyste/paslaugos-internetu/prisijungimo-priemones-smart-id-m-parasas>. Atkreiptinas dėmesys į tai, kad pateiktos nuorodos skiltyje „Prisijungimas prie SEB banko interneto banko“ nurodoma, kad „įvedus teisingą PIN1 kodą, interneto bankas automatiškai atsidarys po kelių sekundžių“, o skiltyje „Mokėjimų ir prašymų tvirtinimas – „įvedus teisingą PIN2 kodą, mokėjimas bus automatiškai patvirtintas po kelių sekundžių“. Lietuvos banko vertinimu, aplinkybė, kad

Taisyklėse SmarID PIN kodų suvedimas nėra atskirai detalizuojamas, o paminėtoje banko interneto svetainėje yra pakankamai aiškiai nurodyta, kad mokėjimo operacijų tvirtinimas yra atliekamas panaudojant SmartID PIN2, taip pat galėjo turėti įtakos, kad pareiškėjas, pirkėju apsimesusio trečiojo asmens prašomas patvirtinti, kaip jis tuo metu manė, lėšų įskaitymo į jo banko sąskaitą operaciją, galėjo nesuprasti, kad SmartID PIN1 kodu tvirtina lėšų nurašymo iš jo banko sąskaitos operaciją.

Įvertinęs pareiškėjo nurodytas aplinkybes, kurių bankas negalėjo paneigti, t. y. pateikti įrodymų, paneigiančių pareiškėjo nurodytas ginčijamos mokėjimo operacijos atlikimo aplinkybes – pareiškėjas neigia autorizavęs tokią mokėjimo operaciją, taip pat atsižvelgdamas į tai, kad paties banko Taisyklėse bei interneto svetainėje viešai skelbiama informacija dėl SmartID PIN kodų naudojimo mokėjimo operacijoms tvirtinti prieštarauja banko argumentams, kad ginčijama mokėjimo operacija turėtų būti laikoma autorizuota paties mokėtojo, Lietuvos bankas nenustatė pakankamo pagrindo teigti, kad ginčijama mokėjimo operacija galėtų būti laikoma atlikta esant pareiškėjo sutikimui (kaip tai suprantama Mokėjimų įstatymo 29 straipsnio 1 dalies kontekste), todėl daro išvadą, kad pareiškėjo ginčijama mokėjimo operacija laikytina neautorizuota.

Dėl neautorizuotos mokėjimo operacijos pasekmių ir pareiškėjo teisės į ginčijamos mokėjimo operacijos sumos gražinimą

Vadovaudamasis Mokėjimų įstatymo 38 straipsnio 1 dalimi, mokėtojo mokėjimo paslaugų teikėjas privalo gražinti mokėtojui 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).

Mokėjimų įstatymo 36 straipsnio 1 dalyje nustatyta mokėtojo mokėjimo paslaugų teikėjo pareiga gražinti mokėtojui neautorizuotos mokėjimo operacijos sumą, jeigu mokėtojas, sužinojęs apie neautorizuotas operacijas, apie tai praneša savo mokėjimo paslaugų teikėjui nedelsdamas, ne vėliau kaip per 13 mėnesių nuo lėšų nurašymo datos. Vadovaujantis Mokėjimų įstatymo 38 straipsnio 1 dalimi, neautorizuota mokėjimo operacija turi būti gražinta mokėtojui nedelsiant, bet ne vėliau kaip iki kitos darbo dienos pabaigos, po to, kai mokėjimo paslaugų teikėjas sužino apie neautorizuotą mokėjimo operaciją.

Mokėjimų įstatymo 37 straipsnio 1 dalyje nustatyta, kad jeigu mokėtojas neigia autorizavęs įvykdytą mokėjimo operaciją ar teigia, kad mokėjimo operacija buvo įvykdyta netinkamai, jo mokėjimo paslaugų teikėjas turi 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; kai mokėtojas neigia autorizavęs įvykdytą mokėjimo operaciją, mokėtojo mokėjimo paslaugų teikėjo arba atitinkamais atvejais mokėjimo inicijavimo paslaugos teikėjo užregistruotas mokėjimo priemonės naudojimas nebūtinai yra pakankamas įrodymas, kad mokėtojas autorizavo mokėjimo operaciją ar veikė nesažiningai arba tyčia ar dėl didelio neatsargumo neįvykdė vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų. Mokėtojo mokėjimo paslaugų teikėjas ir atitinkamais atvejais mokėjimo inicijavimo paslaugos teikėjas turi pateikti įrodymų, kuriais patvirtinamas mokėtojo sukčiavimas arba didelis neatsargumas (Mokėjimų įstatymo 37 straipsnio 3 dalis).

Mokėjimų įstatymo 39 straipsnio 3 dalyje nustatyta, kad mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai, jeigu jis juos patyrė veikdamas nesažiningai arba tyčia arba dėl didelio neatsargumo neįvykdęs vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų. Tokiais atvejais šio straipsnio 1 dalyje nustatytas didžiausias nuostolių sumos ribojimas netaikomas.

Įvertinus pirmiau nurodytas Mokėjimų įstatymo nuostatas, galima teigti, kad mokėtojo mokėjimo paslaugų teikėjas gali būti visiškai atleistas nuo pareigos gražinti 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).

Pažymėtina, kad šalių ginčo dėl to, kad pareiškėjas galėjo veikti nesažiningai arba tyčia, įskaitant sukčiavimą, nėra, todėl darytina išvada, kad galimo sukčiavimo požymių (nesąžiningumo ir (arba) tyčios) pareiškėjo veiksmuose nėra. Taigi, siekiant įvertinti, kam (pareiškėjui ar bankui) tenka dėl ginčijamos mokėjimo operacijos, kuri, kaip minėta prieš tai, Lietuvos banko vertinimu, laikytina neautorizuota, atsiradę nuostoliai, būtina įvertinti, ar

pareiškėjo veiksmuose galėjo būti didelio neatsargumo požymių.

Antrosios mokėjimo paslaugų direktyvos (toliau – PSD2) preambulės 72 punkte rašoma: „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 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).“

Atkreiptinas dėmesys į tai, kad, nors bankas teigia, kad ginčijama mokėjimo operacija buvo autorizuota paties pareiškėjo, tačiau papildomai nurodo, kad, jo vertinimu, inicijuodamas ir tvirtindamas ginčijamą mokėjimo operaciją pareiškėjas elgėsi itin neatsargiai (nerūpestingai), jo neatsargus elgesys galėjo nulemti tai, kad pareiškėjas tretiesiems asmenims atskleidė mokėjimo kortelės duomenis, interneto banko atpažinimo kodą bei SmartID PIN1 kodą, ir tai, kad šie tretieji asmenys atliko ginčijamą mokėjimo operaciją. Banko vertinimu, inicijuodamas ir tvirtindamas ginčijamą mokėjimo operaciją, pareiškėjas elgėsi itin neapdairiai ir neatsargiai, nesilaikė Mokėjimų įstatymo 34 straipsnyje, kuris nustato mokėjimo priemonės naudotojui pareigą naudotis mokėjimo priemone pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, aptartų mokėjimo paslaugų vartotojo pareigų – naudojosi mokėjimo priemone ne pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, t. y. atskleidė mokėjimo kortelės duomenis, interneto banko atpažinimo kodą ir SmartID PIN1 kodą tretiesiems asmenims.

Siekdamas pagrįsti argumentus, kad sukčių pateiktoje interneto svetainėje suveddamas savo asmens duomenis ir mokėjimo kortelės duomenis bei patvirtindamas savo tapatybę SmartID PIN1 kodu, pareiškėjas elgėsi itin nerūpestingai (aplaidžiai), bankas teigia, kad veddamas minėtus duomenis pareiškėjas dėjo nepakankamai pastangų susipažinti su interneto puslapyje, kuriame buvo prašoma suvesti savo asmens duomenis bei mokėjimo kortelės duomenis, pateikiama informacija. Kadangi pareiškėjo ir sukčių susirašinėjimas buvo užsitęsęs, pareiškėjas turėjo pakankamai laiko įvertinti savo veiksmus, vykdomos mokėjimo operacijos paskirtį ir detales bei nutraukti neatsargius veiksmus ir nevykdyti tolimesnių sukčių nurodymų, tačiau jis elgėsi nerūpestingai ir to nepadarė. Nors veddamas minėtus duomenis pareiškėjas suabejojo dėl vykdomos operacijos, tačiau, nepaisydamas to, kad buvo prekės pardavėjas, o ne pirkėjas (mokėtojas), patvirtino mokėjimo operaciją. Nors SmartID klientų aptarnavimo specialistas įspėjo apie galimą sukčiavimo atvejį, tačiau pareiškėjas ir į tai nekreipė dėmesio ir toliau vykdė sukčių nurodymus, be to, būdamas patyręs mokėjimo paslaugų vartotojas, neatkreipė reikiamo dėmesio ir į sukčių prašymą patvirtinti savo asmens tapatybę suvedant banko atpažinimo kodą bei SmartID PIN 1 kodą, nors žinojo, kad šių elementų vedimas reiškia lėšų pervedimo mokėjimo operacijos patvirtinimą. Nors pareiškėjui kilo įtarimų dėl interneto svetainės, į kurią pateko atidaręs tariamo pirkėjo atsiųstą nuorodą, tačiau jis nesusilaikė nuo tolimesnių veiksmų ir nedėjo jokių pastangų patikrinti svetainės saugumą.

Lietuvos banko nuomone, mokėtojo didelis neatsargumas turėtų būti objektyviai aiškus, t. y. pasireikšti esminiu pareigos elgtis rūpestingai pažeidimu ir (arba) atsargumo priemonių nepaisymu, asmens galėjimu numatyti tokio nerūpestingo elgesio pasekmes bei veiksmų išvengti tokių pasekmių nesiėmimu. Kaip jau buvo minėta pirmiau, Mokėjimų įstatymo 34 straipsnyje reglamentuojama viena iš mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigų – naudotis mokėjimo priemone pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas. Banko Lietuvos bankui pateiktos banko ir pareiškėjo 2018 m. gegužės 13 d. sudarytos SEB Mylimiausia MasterCard (debeto) kortelės sutarties (toliau – Sutartis) ir jos sudedamosios dalies Mokėjimo kortelių išdavimo ir naudojimo taisyklių 4.1.7 papunktyje reglamentuojama, kad kortelės turėtojas privalo „laikyti, kad *sandoris, už kurį kortele atsiskaityta iš sąskaitos*, įvyko, jei Kortelės turėtojas pasirašė operaciją kortele liudijančiame dokumente arba *nurodė kortelės numerį, užsakydamas prekes ar paslaugas telefonu, paštu ar internetu* (nepateikdamas pačios kortelės) ir *įvedė mobiliuoju telefonu ar elektroniniu paštu gautą vienkartinį saugos kodą, jeigu prekybininkas / paslaugos*

teikėjas dalyvauja programose „Verified by Visa“ arba „MasterCard SecureCode“ arba naudojosi PIN kodu imdamas grynujų pinigų iš bankomatų / įmokėdamas grynuosius pinigus į bankomatus ar atsiskaitydamas lustine kortele aptarnavimo vietose, kuriose yra įrengtas lustinių kortelių skaitytuvas; laikyti, kad Kortelės turėtojas (Klientas), paslaugos teikėjui pateikęs kortelės duomenis internetu bei įvedęs mobiliuoju telefonu ar elektroniniu paštu gautą vienkartinį saugos kodą, jeigu prekybininkas / paslaugos teikėjas dalyvauja programose „Verified by Visa“ arba „MasterCard SecureCode“, patvirtino įsipareigojimą sumokėti už prekes ar paslaugas iš sąskaitos pagal operaciją kortele liudijantį dokumentą. (4.1.8. papunktis); atsiskaitydamas kortele internetu, elektroninės parduotuvės reikalavimu nurodyti kortelės CVV2/CVC2 kodą (4.1.9 papunktis).“

Kaip matyti iš pirmiau aptartų Sutarties nuostatų, jose yra aiškiai ir nedviprasmiškai nustatyta, kad mokėjimo kortelės duomenų pateikimas paslaugos teikėjui reiškia mokėtojo patvirtinimą įsipareigoti sumokėti už prekes ar paslaugas iš su kortele susietos banko sąskaitos. Taigi, pareiškėjas turėjo suprasti (numatyti), kad kortelės duomenų pateikimas (kortelės numeris, galiojimo data, CVC kodas) yra skirtas lėšų nurašymo iš sąskaitos operacijai inicijuoti, o ne lėšoms į sąskaitą įskaityti. Banko pateiktais duomenimis, pareiškėjas turėjo patirties inicijuojant mokėjimo operacijas kortele bei tvirtinant tapatybę SmartID PIN1. Nors, kaip buvo minėta anksčiau, banko Taisyklėse SmartID PIN kodų suvedimas nėra atskirai detalizuojamas, o banko interneto svetainėje yra pakankamai aiškiai aprašyta, kad mokėjimo operacijų tvirtinimas yra atliekamas panaudojant SmartID PIN2, tačiau pareiškėjui turėjo sukelti įtarimų vien faktas, kad jo buvo prašoma suvesti mokėjimo kortelės duomenis bei SmartID PIN1, nors pareiškėjas pats neturėjo tikslo inicijuoti lėšų pervedimo operacijos, o tenorėjo gauti lėšas į sąskaitą. Pareiškėjas galėjo ir turėjo žinoti (suprasti), kad lėšų gavimo į banko sąskaitą mokėjimo operacijai nereikia suvesti mokėjimo kortelės duomenų bei patvirtinti savo tapatybės suvedant SmartID PIN1.

Pareiškėjui turėjo kilti įtarimų ir tuomet, kai, tvirtinant, kaip pareiškėjas tuo metu manė tvirtinantis, lėšų gavimo į sąskaitą operaciją, buvo prašoma suvesti savo banko sąskaitos likutį, nes atliekant mokėjimo operacijas prie mokėjimo operacijai inicijuoti reikalingos nurodyti informacijos niekada nėra prašoma įvesti duomenų apie banko sąskaitos likutį.

Remiantis pareiškėjo paaiškinimais apie ginčijamos mokėjimo operacijos atlikimo aplinkybes, o būtent tuo, kad pareiškėjas teigia, kad, veddamas savo asmens duomenis, kortelės duomenis, banko atpažinimo kodą bei SmartID PIN1, dirbo kitus darbus, todėl nebuvo atidus (nors, kaip teigia, neturėjo prekybos internetu patirties, tačiau turėjo patirties atsiskaitant kortele), nors jam kilo įtarimų dėl trečiųjų asmenų prašomų atlikti veiksmų, pareiškėjas ir toliau vykdė trečiųjų asmenų nurodymus nesistengdamas patikrinti informacijos, kad būtų išsklaidyti kilę įtarimai, galima teigti, kad pareiškėjas nesielgė kaip rūpestingas vartotojas. Pareiškėjas trečiųjų asmenų nurodymus vykdė net ir tuomet, kai pastebėjo, kad asmens, kuris tariamai pareiškėjui į banko sąskaitą turi pervesti 15 Eur, vardas ir pavardė sukčių pateiktoje aplinkoje skyrėsi nuo pirkėjo, su kuriuo pareiškėjas derėjosi dėl prekės pardavimo, vardo ir pavardės, tuomet, kai pareiškėją apie galimą sukčiavimo atvejį įspėjo SmartID darbuotojas, tuomet, kai jo buvo prašoma suvesti duomenis, kurie buvo reikalingi lėšų nurašymo mokėjimo operacijai kortele inicijuoti: mokėjimo kortelės duomenis, savo banko sąskaitos likutį bei SmartID PIN1.

Iš ginčo byloje pateiktų duomenų galima teigti, kad pareiškėjas, nors ir numatė galimą trečiųjų asmenų sukčiavimą, bet vis tiek nesiėmė jokių atsargumo priemonių, nesistengė panaikinti abejonių, įsiklausyti į kitų asmenų įspėjimus apie galimą sukčiavimą, priešingai – ir toliau tęsė savo itin neatsargius veiksmus, kurie galiausiai lėmė mokėjimo priemonės praradimą ir lėšų nurašymą iš pareiškėjo sąskaitos.

Lietuvos banko vertinimu, visos pirmiau minėtos aplinkybės leidžia teigti, kad pareiškėjo elgesys buvo labai neatsargus. Nors galėjo numatyti, kad pateikdamas mokėjimo kortelės duomenis inicijuoja lėšų nurašymo iš sąskaitos operaciją, turėdamas įtarimų bei perspėjimų dėl galimo sukčiavimo, pareiškėjas nesiėmė jokių atsargumo priemonių, priešingai, net ir įtardamas sukčiavimą, vykdė trečiųjų asmenų nurodymus ir sudarė galimybes tretiesiems asmenims pasisavinti pareiškėjo mokėjimo priemonę. Toks išskirtinai neatsargus pareiškėjo elgesys gali būti vertinamas kaip didelis neatsargumas, lėmęs pinigų iš pareiškėjo sąskaitos pervedimą tretiesiems asmenims, todėl ir visi dėl neautorizuotos ginčijamos mokėjimo operacijos patirti nuostoliai turėtų tekti pareiškėjui.

Įvertinus pirmiau išdėstytą informaciją, konstatuotina, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, nustatančią, kad mokėtoju tenka visi dėl neautorizuotų

mokėjimo operacijų atsiradę nuostoliai, jeigu jis juos patyrė dėl didelio neatsargumo neįvykdęs vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų, todėl, Lietuvos banko vertinimu, bankas neturi pareigos pareiškėjui gražinti neautorizuotos mokėjimo operacijos lėšų.

Dėl ginčijamos mokėjimo operacijos ginčo procedūros tarptautinėje mokėjimų kortelių organizacijoje „MasterCard“

Pareiškėjas teigia, kad bankas neėjo pakankamai pastangų, kad būtų sugražintos ginčijamos mokėjimo operacijos lėšos. Bankas teigia, kad, vadovaujantis „MasterCard“ kortelių asociacijos taisyklėmis, bankas negali pradėti ginčijamos mokėjimo operacijos ginčo procedūros dėl lėšų sugražinimo, nes mokėjimas buvo atliktas ne prekybininkui, o pervedimui tarpininkui *Walletatabu_int_in*, kuris lėšas pavedė galutiniam lėšų gavėjui – *duomenys neskelbiami*. Bankas paaiškino, kad pagal veiklos kodą (6538) *Walletatabu_int_in* teikia pinigų pervedimo paslaugas (*MoneySend Funding*), tai reiškia, kad jo įsipareigojimas – atlikti pareiškėjo suformuotą ir patvirtintą mokėjimą – buvo įvykdytas. Banko teigimu, atsižvelgiant į tai, kad paslauga – pinigų pervedimas – buvo suteikta, vadovaujantis „MasterCard“ taisyklėmis, bankas neturi teisės pradėti mokėjimo operacijos ginčo procedūros.

Bankas yra pateikęs „MasterCard“ organizacijai paklausimą dėl galimybės ginčyti prekybininkų (užsiimančių lėšų pervedimu ar labdara) kaip galimai neteisėtas („fraud“) operacijas, tačiau „MasterCard“ patvirtino, kad ginčyti tokių mokėjimo operacijų kaip neteisėtų, t. y. atliktų be kliento žinios, nėra galimybės ir ginčo procedūra nėra leidžiama.

Vertinant banko civilinės atsakomybės klausimą dėl galbūt netinkamo atstovavimo pareiškėjui „MasterCard“ asociacijoje, svarbu pažymėti, kad papildomas galimybes kortelės turėtojui susigražinti pinigines lėšas nustato „MasterCard“ taisyklės, nei Lietuvos Respublikos teisės aktai, nei Europos Sąjungos teisės aktai nereglamentuoja, kokiomis sąlygomis turi būti vykdomos lėšų gražinimo procedūros (angl. *chargeback*). Taip pat banko ir pareiškėjo sudarytos sutarties nuostatos nereglamentuoja banko teisių ir pareigų atstovaujant kortelės turėtojui (pareiškėjui) mokėjimo operacijos ginčo procedūroje tarptautinėse mokėjimo kortelių organizacijose.

Taigi, banko veiksmus ginčijant mokėjimo operacijas reglamentuoja „MasterCard“ taisyklės. Bankas Lietuvos bankui pateikė „MasterCard“ asociacijos taisyklių sąlygų, kuriomis remiasi nepradėdamas mokėjimo operacijos ginčo procedūros, ištrauką, joje nurodyta, kad mokėjimo operacijos ginčo procedūra „MasterCard“ asociacijoje gali būti pradėta kaip atlikta be mokėtojo žinios, jeigu mokėjimo operacija nėra patvirtinta *3D secure* kodu. Bankas Lietuvos bankui pateikė kopiją „MasterCard“ asociacijos elektroninio laiško, kuriame „MasterCard“ asociacijos teiraujamas, ar yra galimybė pradėti ginčo procedūrą dėl mokėjimo operacijų, kurios yra patvirtintos *3D secure* kodu, tačiau mokėtojas neigia davęs sutikimą jas atlikti. Remiantis minėtame laiške pateiktu „MasterCard“ asociacijos išaiškinimu, ginčo procedūra dėl tokių mokėjimo operacijų pagal „MasterCard“ asociacijos taisykles nėra leidžiama.

Iš Lietuvos bankui pateiktų duomenų, Lietuvos bankas neturi pagrindo teigti, kad bankas netinkamai taikė lėšų gražinimo procedūrą (*chargeback*) ir dėl to lėšos pareiškėjui nebuvo sugražintos.

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 ginčo sprendimo kreiptis į teismą arba kitą ginčų nagrinėjimo instituciją įstatymų nustatyta tvarka. Kreipimasis į teismą po Lietuvos banko sprendimo dėl ginčo esmės priėmimo nelaikomas šio sprendimo apskundimu.