



**LIETUVOS BANKO
TEISĖS IR LICENCIJAVIMO DEPARTAMENTO
DIREKTORIUS**

**SPRENDIMAS
DĖL X. X. IR BANKO LUMINOR BANK AS GINČO NAGRINĖJIMO**

2022 m. gegužės 19 d. Nr. 429-185
Vilnius

Lietuvos bankas gavo X. X. (toliau – pareiškėjas) atstovės advokatės Y. Y. (toliau – pareiškėjo atstovė) kreipimąsi, kuriuo prašoma išnagrinėti tarp pareiškėjo ir banko *Luminor Bank AS*, veikiančio per Lietuvoje įsteigtą filialą, (toliau – bankas) kilusį ginčą.

N u s t a t y t a:

2022 m. sausio 20 d., panaudojus pareiškėjo mokėjimo kortelės *Visa Debit* Nr. (*duomenys neskelbtini*) (toliau – mokėjimo kortelė) duomenis, buvo atliktos 3 mokėjimo operacijos: 1 050 Eur ir 1 680 Eur mokėjimai gavėjui *MUCHBETTER SOUTHEND* ir 260,87 Eur mokėjimas (8 144,00 Ukrainos grivinos valiuta – UAH) gavėjui *MONO-BANK Kiev UAMONOF* (toliau – Ginčijami mokėjimai).

Tą pačią dieną pareiškėjas kreipėsi telefonu į banką ir pranešė apie Ginčijamus mokėjimus, informuodamas, kad lėšos su mokėjimo kortele susietoje sąskaitoje yra rezervuotos, nes sukčiai galėjo pasinaudoti jo mokėjimo kortelės duomenimis. Pokalbio metu pareiškėjo mokėjimo kortelė buvo užblokuota, o pareiškėjas buvo informuotas, kad apie galimą sukčiavimo atvejį turi pranešti teisėsaugos institucijoms ir užpildyti paraiškas interneto banke, prašant išnagrinėti galimybę Ginčijamų mokėjimų lėšas gražinti.

2022 m. sausio 21 d. pareiškėjas pateikė prašymus bankui atšaukti lėšų rezervaciją Ginčijamiems mokėjimams įvykdyti.

2022 m. sausio 21 d. bankas, interneto banko žinute atsakydamas į pareiškėjo prašymus, nurodė, kad atlikus tyrimą nustatyta, jog Ginčijami mokėjimai buvo patvirtinti tik pareiškėjui žinomą internetinės bankininkystės autentifikavimo saugos kodu, todėl bankas šių operacijų ginčyti negali. Bankas pasiūlė pareiškėjui dėl lėšų rezervacijos panaikinimo kreiptis į paslaugos (prekės) tiekėją.

2022 m. sausio 23 d. gavus patvirtinimą iš lėšų gavėjo banko apie įvykdytus Ginčijamus mokėjimus, lėšos iš pareiškėjo su mokėjimo kortele susietos sąskaitos buvo nurašytos.

Pareiškėjas nesutinka su banko sprendimu negražinti Ginčijamų mokėjimų lėšų. Pareiškėjo atstovės pateiktame kreipimesi nurodoma, kad 2022 m. sausio 14 d. pareiškėjas internetiniame skelbimų puslapyje „Skelbiu.lt“ įkėlė skelbimą, siekdamas parduoti jam priklausantį vaikišką keturratį, o 2022 m. sausio 20 d. apie 14:53 val. iš nenustatyto asmens programėlėje „WhatsApp“ gavo pranešimą apie „Omniva“ paštomate apmokėtą pareiškėjo parduodamą prekę. Paspaudus pirkėjo pranešime pateiktą nuorodą, siekiant gauti lėšas į savo sąskaitą, atsiradusiame pašto siuntų bendrovės „Omniva“ interneto puslapyje buvo prašoma pateikti mokėjimo kortelės duomenis – vardą, pavardę ir kortelės numerį. Sistemai nurodžius, kad pirmoji pareiškėjo pateikta (kito mokėjimo paslaugų teikėjo išduota) kortelė yra netinkama, pareiškėjas apie 15:55 val. suvedė banko išduotos mokėjimo kortelės duomenis – mokėjimo kortelės numerį. Kreipimesi teigiama, kad, suvedęs mokėjimo kortelės numerį, pareiškėjas pastebėjo, kad vykdoma mokėjimo operacija, todėl nedelsdamas prisijungė prie savo interneto banko ir apie 15:56 val. pamatė, kad jo su mokėjimo kortele susietoje sąskaitoje buvo įvykdytos 3 mokėjimo operacijos – Ginčijami mokėjimai, kurioms įvykdyti rezervuota 2 990,87 Eur suma. Supratęs buvęs apgautas, pareiškėjas nurodo nedelsdamas paskambinęs į banką ir paprašęs užblokuoti jo mokėjimo kortelę ir atšaukti Ginčijamus mokėjimus. Pareiškėjas teigia, kad banko darbuotojos buvo patikintas, kad rezervuotos lėšos nebus nurašytos, o saugomos jo sąskaitoje iki 2022 m. sausio 29 d., jam buvo patarta dėl Ginčijamų mokėjimų atšaukimo kreiptis į banką raštu per interneto banką. Vykdydamas banko darbuotojos nurodymus,

pareiškėjas teigia tą pačią dieną interneto banke pateikęs prašymą bankui dėl Ginčijamų mokėjimų atšaukimo, taip pat apie įvykį pranešė policijai, ji pradėjo ikiteisminį tyrimą. Kitą dieną pareiškėjas nurodo gavęs banko atsakymą, kad bankas negali gražinti Ginčijamų mokėjimų lėšų, todėl pataria pareiškėjui dėl Ginčijamų mokėjimų atšaukimo kreiptis į paslaugos ar prekės teikėją. Su šia banko pozicija pareiškėjas nesutinka ir teigia, kad Ginčijamų mokėjimų inicijavimo metu jis nesinaudojo jokiais internetinės bankininkystės autentifikavimosi saugos priemonėmis, pareiškėjas taip pat nurodo nesuvedęs mokėjimo kortelės CVV kodo, būtino atlikti mokėjimo operacijas kortele. Tai, kad Ginčijami mokėjimai, „suvedus tik mokėjimo kortelės numerį“, buvo įvykdyti ir šių mokėjimų lėšos buvo pervestos nusikalstamu būdu Ginčijamus mokėjimus inicijavusiems asmenims, pareiškėjo atstovės teigimu, pagrindžia teiginį, kad banko sistemose yra saugumo spragų¹. Kreipimesi taip pat teigiama, kad bankas, sužinojęs apie Ginčijamus mokėjimus, nesiėmė jokių veiksmų tam, kad pareiškėjo neautorizuoti Ginčijami mokėjimai būtų atšaukti, taigi, leido nusikalstamą veiką įvykdžiusiems asmenims pasisavinti pareiškėjo lėšas. Pareiškėjo atstovė mano, kad dėl banko aplaidžių veiksmų pareiškėjas patyrė 2 990,87 Eur nuostolių, todėl, nustatčius visas banko civilinės atsakomybės sąlygas, bankas turėtų atlyginti pareiškėjo nuostolius dėl įvykdytų Ginčijamų mokėjimų. Kreipimesi Lietuvos banko prašoma rekomenduoti bankui kompensuoti pareiškėjui Ginčijamų mokėjimų lėšas – 2 990,87 Eur.

Bankas nesutinka tenkinti pareiškėjo reikalavimo. Atsiliepime teigiama, kad bankas mokėjimo kortelių operacijų patvirtinimo užklausas gauna ir jas vykdo pagal tarptautinės mokėjimo kortelių organizacijos „Visa“ nustatytas taisykles ir rezervuoja lėšas mokėjimo kortelės sąskaitoje, gavęs atitinkamą užklausa, o lėšas nurašo tik vėliau gavęs paslaugos (prekės) tiekėjo banko patvirtinimą. Aptariamam atveju, banko teigimu, gautos užklaustos rezervuoti lėšas pateiktos tinkamai, be to, Ginčijami mokėjimai papildomai patvirtinti identifikuojant kortelės turėtoją jo pasirinktu saugesniu autentifikavimo metodu. Bankas pažymėjo, kad patvirtinti mokėjimai mokėjimo kortele negali būti atšaukti ar nevykdomi, kai gaunami atitinkami duomenys iš operacijos atlikimo vietos, t. y. prekės ar paslaugos tiekėjo, iš kurio banko klientas kortele perka prekes ar paslaugas ir bankui pateikia patvirtinimą apie atsiskaitymą kortele. Atšaukti mokėjimo nurodymus bei panaikinti lėšų rezervacijas gali inicijuoti tik paslaugos ar prekės tiekėjas, nes jis, kaip nurodoma atsiliepime, informuoja banką, ar su kortele susietos banko sąskaitos savininkas atsiskaitė kortele, pirkdamas prekes ar paslaugas, ar atsiskaitymo neatliko. Būtent todėl, banko teigimu, pareiškėjui atsakyme į jo prašymą gražinti Ginčijamų mokėjimų lėšas buvo nurodyta kreiptis į lėšų gavėjus dėl šių mokėjimo operacijų atšaukimo.

Banko vertinimu, atsižvelgiant į tai, kad pareiškėjas pripažino savo valia atskleidęs mokėjimo kortelės duomenis kitiems asmenims, laikytina, kad jis veikė neatsargiai ir neapdairiai ir neapsaugojo savo mokėjimo priemonės personalizuotų saugumo duomenų. Bankas teigia įvertinęs pareiškėjo Ginčijamus mokėjimus ir nustatęs, kad jie buvo tinkamai autorizuoti, t. y. pagal banko mokėjimo paslaugų teikimo sąlygų reikalavimus, taikant saugesnį autentiškumo patvirtinimą: Ginčijami mokėjimai buvo atlikti, suvedus mokėjimo kortelės duomenis (žinojimo elementas) ir patvirtinus operacijas „Smart-ID“ programėle (turėjimo elementas). Bankas papildomai pažymi, kad naudojantis interneto banko prisijungimo priemone patvirtintų mokėjimo kortele atliktų operacijų bankas ginčyti negali pagal „Visa“ mokėjimo kortelių organizacijos taisykles, todėl bankas ir šiuo atveju Ginčijamų mokėjimų užginčyti ir inicijuoti tarptautinio tyrimo neturėjo galimybes. Remdamasis atsiliepime išdėstytais argumentais, bankas prašo atmesti pareiškėjo reikalavimą kaip nepagrįstą.

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

Vadovaujantis Lietuvos banko valdybos 2012 m. sausio 26 d. nutarimu Nr. 03-23 patvirtintų Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių (toliau – Taisyklės) 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. Vykstant ginčo nagrinėjimo procesui Lietuvos bankas neatlieka Lietuvos Respublikos Lietuvos banko įstatymo 42¹ straipsnyje

¹ Nors pareiškėjo atstovės pateiktame kreipimesi pripažįstama, kad suklastotoje interneto svetainėje buvo prašoma suvesti mokėjimo kortelės turėtojo vardą, pavardę, kortelės numerį, tačiau kartu teigia, kad mokėjimo kortelės numerio užteko, kad būtų įvykdyti Ginčijami mokėjimai. Vis dėlto pats pareiškėjas tiek savo paties pateiktame kreipimesi Lietuvos bankui, tiek papildomuose paaiškinimuose pripažįsta atskleidęs ir savo vardą bei pavardę.

reglamentuojamų patikrinimų, skirtų faktinėms aplinkybėms, susijusioms su Lietuvos banko prižiūrimo finansų rinkos dalyvio galbūt padarytais teisės aktų reikalavimų pažeidimais, nustatyti ir vertinti. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Pareiškėjo ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjui Ginčijamų mokėjimų sumas, iš pareiškėjo su mokėjimo kortele susietos sąskaitos nurašytas, įvykus sukčiavimo atakai. Pareiškėjas neigia autorizavęs Ginčijamus mokėjimus, taip pat mano, kad Ginčijami mokėjimai buvo įvykdyti dėl to, kad banko sistemose yra saugumo spragų. Bankas teigia, kad tretieji asmenys įgijo sąlygas inicijuoti Ginčijamus mokėjimus tik todėl, kad pareiškėjas dėl didelio neatsargumo atskleidė savo mokėjimo kortelės personalizuotus saugumo duomenis tretiesiems asmenims. Bankas, remdamasis vidinės sistemos duomenimis, pagrindžiančiais, kad Ginčijami mokėjimai buvo patvirtinti pareiškėjo naudojama tapatybės patvirtinimo priemone, mano, kad Ginčijamų mokėjimų, kurie, banko vertinimu, buvo tinkamai autorizuoti, sumų pareiškėjui neturi pareigos grąžinti ir (ar) kompensuoti.

Lietuvos banko vertinimu, siekiant išspręsti pareiškėjo ir banko ginčą bei pasisakyti dėl pareiškėjo keliamo reikalavimo pagrįstumo, visų pirma, būtina nustatyti, ar pareiškėjo Ginčijami mokėjimai laikytini autorizuotais, t. y. ar pareiškėjas davė sutikimą atlikti Ginčijamus mokėjimus. Įvertinus Ginčijamų mokėjimų patvirtinimo (autorizavimo) aplinkybes, spręstinas klausimas ir dėl banko atsakomybės grąžinti ir (ar) kompensuoti pareiškėjui Ginčijamų mokėjimų sumą. Atsižvelgus į pareiškėjos kreipimesi dėstomus argumentus, taip pat vertintinas banko sistemų saugumas ir banko veiksmų pagrįstumas, atsisakant atšaukti mokėjimo nurodymus įvykdyti Ginčijamus mokėjimus ar inicijuoti dėl jų lėšų grąžinimo procedūras.

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

Dėl Ginčijamų mokėjimų 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 įstatymo 37 straipsnio 1 dalyje nustatyta, kad tuo atveju, 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.

Pažymėtina, kad Mokėjimų įstatyme nėra nustatytų konkrečių mokėtojo sutikimo įvykdyti mokėjimo operaciją būdų ir (arba) išsamios 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 mokėjimo paslaugų teikimo sąlygų 11.9 papunktyje nustatyta, kad „mokėjimo operacija laikoma autorizuota tik tada, kai Klientas duoda sutikimą ją vykdyti. Šio sutikimo davimo forma ir tvarka nustatoma sutartyje. Klientas gali autorizuoti mokėjimo operaciją iki jos įvykdymo arba ją įvykdęs, jeigu taip susitarė Klientas ir Bankas. Jeigu pirmiau nurodyto sutikimo nėra, laikoma, kad mokėjimo operacija yra neautorizuota.“ Vadovaujantis banko mokėjimo paslaugų teikimo sąlygų 6.3.1 papunkčio, nurodančio, kokiais būdais banko klientas gali pateikti sutikimą atlikti operaciją, nuostatomis, „Klientas sutikimą atlikti mokėjimo operaciją gali pateikti Banko nustatyta arba Banko ir Kliento sutarta forma ir būdu. <...> Sutikimas dėl mokėjimo operacijų taip pat gali būti tvirtinamas naudojant Kliento atpažinimo priemonės ir / ar kitais Bankui priimtinais būdais / priemonėmis. Atsiskaitant kortele, tam tikrais

atvejais, kortelės turėtojas sutikimą atlikti mokėjimo operaciją taip pat gali patvirtinti pateikdamas kortelės duomenis ar nustatytu eiliškumu atlikdamas tam tikrus veiksmus (kortelės įdėjimas į tam skirtą vietą, kortelės prigludimas prie specialių ženklų pažymėto kortelių aptarnavimo skaitytuvo, konkrečios paslaugos ar prekės užsakymas), kurie jam siūlomi savitarnos ir kitose atsiskaitymo vietose. <...> Visais šiame punkte nurodytais būdais patvirtintas sutikimas atlikti mokėjimo operaciją ar dokumentai, laikomi patvirtintais Kliento ir / ar kortelės turėtojo (kortelės operacijų atveju) ir turinčiais tokią pat teisinę galią kaip ir Kliento ir / ar kortelės turėtojo (kortelės operacijų atveju) pasirašyti popieriniai dokumentai."

Nors pirmiau aptartomis banko mokėjimo paslaugų teikimo sąlygų nuostatomis taip pat remiasi bankas, norėdamas pagrįsti teiginį, kad Ginčijami mokėjimai buvo tinkamai, t. y. šalių sutartu būdu, autorizuoti, būtina pažymėti, kad minėtose nuostatose kalbama apie atvejus, kai mokėtojas duoda savo sutikimą pervesti lėšas ir tuo tikslu panaudoja jam išduotas mokėjimo ir tapatybės patvirtinimo priemones. Tačiau nagrinėjamo ginčo atveju, priešingai, nei nurodyta aptariamose nuostatose, pareiškėjas savo mokėjimo kortelės personalizuotus saugumo duomenis panaudojo fiktyvioje – į mobiliąją pokalbių programėlę gautą nuorodą paspaudus atsiradusioje, interneto svetainėje ir juos suvedė ne dėl to, kad ketino pervesti lėšas, siekdamas atsiskaityti už suteiktas paslaugas ar įsigytas prekes, o vykdydamas gautoje žinutėje pateiktus nurodymus ir siekdamas patvirtinti lėšų gavimą į banke esančią ir su mokėjimo kortele susietą savo sąskaitą už parduodamą prekę. Taigi, pareiškėjas, tiek bendraudamas su banku dėl Ginčijamų mokėjimų, tiek ir kreipimesi į Lietuvos banką nuosekliai laikosi pozicijos, kad valios inicijuoti ir įvykdyti Ginčijamus mokėjimus jis neišreiškė ir nedavė tam savo sutikimo – neautorizavo Ginčijamų mokėjimų šalių sutarta forma ir tvarka. Be to, tiek pareiškėjas, tiek pareiškėjo atstovė ne kartą pažymėjo, kad pareiškėjas suklastotoje interneto svetainėje suvedė tik mokėjimo kortelės numerį, o kitų mokėjimo kortelės personalizuotų saugumo duomenų (konkrečiai – mokėjimo kortelės CVV kodo) jis niekur nesuvedė ir niekam neatskleidė, pareiškėjas taip pat neigia Ginčijamų mokėjimų inicijavimo metu naudojęs turimą tapatybės patvirtinimo priemonę „Smart-ID“ ir (ar) suvedęs savo „Smart-ID“ paskyros PIN1 kodą.

Darydamas išvadą, kad Ginčijami mokėjimai buvo autorizuoti šalių sutarta tvarka, bankas iš esmės remiasi tik tuo faktu, kad, banko vidinės sistemos duomenimis, Ginčijamiems mokėjimams įvykdyti buvo panaudoti mokėjimo kortelės duomenys ir suvestas pareiškėjo „Smart-ID“ paskyros PIN1 kodas, tačiau, darydamas tokią išvadą, bankas nevertino, kada, kaip ir (arba) kas perdavė lėšų gavėjui ir (arba) jo mokėjimo paslaugų teikėjui duomenis, kurių pagrindu buvo inicijuoti Ginčijami mokėjimai, t. y. ar šiuos duomenis tiesiogiai pateikė pats pareiškėjas, ar iš pareiškėjo šiuos duomenis neteisėtai išvilioję tretieji asmenys. Bankas kartu su atsiliepimu pateikė jo vidaus sistemose užfiksuotus duomenis, pagrindžiančius, kad inicijuojant Ginčijamus mokėjimus buvo suvestas mokėjimo kortelės CVV kodas ir Ginčijami mokėjimai papildomai patvirtinti identifikuojant mokėjimo kortelės turėtoją (šiuo atveju – pareiškėją) jo pasirinktu autentifikavimo metodu, t. y. suvedus tik pareiškėjui žinomą jo naudojamos tapatybės patvirtinimo priemonės „Smart-ID“ paskyros PIN1 kodą, taip pat duomenis, kad galinis įrenginys (pagal jo IP adresą), iš kurio, naudojantis „Smart-ID“ programėle, patvirtinti Ginčijami mokėjimai, yra pareiškėjo įprastai naudojamas galinis įrenginys, jungiantis prie interneto banko. Vis dėlto, Lietuvos banko vertinimu, vien šie duomenys dar savaime neįrodo, kad Ginčijami mokėjimai iš tiesų atlikti su pareiškėjo sutikimu (pareiškėjas išreiškė savo valią). Kaip minėta pirmiau, remiantis Mokėjimų įstatymo nuostatomis, vien aplinkybė, kad mokėtojo mokėjimo paslaugų teikėjo vidaus sistemose užregistruotas mokėtojai išduotas mokėjimo priemonės, įskaitant jos personalizuotus saugumo duomenis, naudojimas, nebūtinai yra pakankamas įrodymas, jog mokėjimo priemone naudojosi ir (arba) mokėjimo operaciją autorizavo pats mokėtojas (Mokėjimų įstatymo 37 straipsnio 3 dalis).

Todėl, Lietuvos banko nuomone, analizuojamų aplinkybių kontekste sprendžiant, ar Ginčijamos mokėjimo operacijos laikytinos autorizuotomis, būtina nustatyti, ar pareiškėjas, kaip pats pripažįsta, suklastotoje interneto svetainėje pateikdamas tam tikrus mokėjimo kortelės duomenis, tikėdamasis, kad taip tvirtinamas lėšų gavimas į sąskaitą, suprato, kad iš tiesų atlieka veiksmus, kurie vėliau gali lemti lėšų nurašymą iš jo su mokėjimo kortele susietos sąskaitos. Taigi, svarbu įvertinti, ar faktinės Ginčijamų mokėjimų patvirtinimo aplinkybės, kurias pagrindžia ginčo byloje esantys duomenys, atitiko ginčo šalių sudarytoje sutartyje aptartą mokėjimo operacijų autorizavimo tvarką.

Norėdamas pagrįsti teiginį, kad nesiekė Ginčijamų mokėjimų inicijavimo ir jų neautorizavo, pareiškėjas kartu su kreipimusi pateikė savo mobiliojo telefono ekrano vaizdo

įrašą, kuriame matyti, kas buvo rodoma pareiškėjui, jam paspaudus pokalbių programėlėje „WhatsApp“ pirkėju prisistačiusio asmens atsiųstą nuorodą. Minėtame pareiškėjo mobiliojo įrenginio ekrano vaizdo įrašė rodomi interneto svetainės, kurioje pareiškėjas turėjo suvesti prašomus pateikti duomenis, kad patvirtintų tariamą lėšų įskaitymą į banke esančią sąskaitą, vaizdai. Pareiškėjo pateikti vaizdiniai duomenys leidžia teigti, kad aptariama fiktyvi interneto svetainė sukuria tikrumo įspūdį: joje naudojamas pašto siuntų bendrovės „Omniva“ originaliam (autentiškam) identiškas prekės ženklas, nurodoma, kad „Gavėjas jau pervedė lėšas“, ir prašoma pateikti pareiškėjo (kaip nurodoma „siuntėjo“) asmens duomenis, siekiant „Gauti lėšas“. Be kita ko, prie dalies „Elemento aprašymas“ pažymima, kad „Aprašymas“ – „vaikiškas elektrinis keturratis“, „Kaina“ – „280 Eur“. Taigi, galima pagrįstai teigti, kad paspaudus nuorodą atsidariusiame interneto puslapyje pateikti duomenys ir matomi vaizdai galėjo pareiškėjui sukurti pirminį įspūdį, kad pirkėju prisistatęs asmuo iš tiesų siekia įsigyti pareiškėjo siūlomą prekę ir tuo tikslu jau yra atlikęs mokėjimą pareiškėjo naudai.

Norėdamas pagrįsti savo poziciją, kad Ginčijami mokėjimai buvo tinkamai autorizuoti, Lietuvos bankui pateiktuose papildomuose paaiškinimuose bankas nurodo, kad, identifikacijai pasirinkus „Smart-ID“ programėlę, mokėjimo kortelės savininkas yra nustatomas naudojant šios tapatybės patvirtinimo priemonės paskyros PIN1 kodą: tokiais atvejais „Smart-ID“ programėlėje yra rodomas operacijos kontrolinis kodas, jis turi sutapti su kontroliniu kodu, kurį mokėtojas mato banko autentifikavimo lange. Banko teigimu, neišitikinus, kad operacijos ir „Smart-ID“ programėlėje rodomi kontroliniai kodai sutampa, „patvirtinti operacijos negalima“. Paaiškindamas šį savo teiginį, bankas nurodė, kad banko klientai, atsiskaitydami už prekes ar paslaugas internetu, panaudojant mokėjimo kortelės duomenis, iš pardavėjo ar paslaugos teikėjo puslapio yra nukreipiami į banko interneto banko puslapį, kuriame rodomas standartinio turinio pranešimas su personalizuotais mokėtojo ir jo inicijuoto mokėjimo nurodymo duomenimis: lėšų gavėjo pavadinimu, suma, mokėjimo kortelės paskutiniai 4 skaitmenimis ir kontroliniu kodu. Bankas nurodo, kad klientas, banko interneto banke rodomame pranešime apie inicijuotą mokėjimo operaciją paspaudęs mygtuką „Patvirtinti“, prieš patvirtindamas operaciją savo naudojamose „Smart-ID“ programėlėje paskyros PIN1 kodu, turi įsitikinti, kad mokėjimo operacijos lange rodomas kontrolinis kodas sutampa su programėlės „Smart-ID“ lange rodomu kontroliniu kodu.

Vis dėlto, remiantis banko paaiškinimais, be kontrolinio kodo, kurį turi sutikrinti mokėtojas tvirtindamas per gavėją inicijuotą mokėjimo operaciją, nėra atliekami jokie kiti veiksmai ir mokėtoju, be banko interneto banke operacijos lange nurodytų duomenų, papildomai nėra rodoma jokia informacija, susijusi su inicijuota mokėjimo operacija. Tad mokėtoju, pasirinkusiam „Smart-ID“, kaip tapatybės patvirtinimo priemonę, rodomas pranešimas, kad reikia suvesti „Smart-ID“ paskyros PIN1 kodą, tačiau nėra rodoma jokia papildoma informacija, susijusi su lėšų gavėju, suma ir pan. Taigi, tokiu atveju (tvirtinant mokėjimą, inicijuotą panaudojus mokėjimo kortelės duomenis) mokėtoju nėra rodoma, kokiu konkrečiu tikslu jo prašoma suvesti tapatybės patvirtinimo priemonės „Smart-ID“ paskyros PIN1 kodą.

Būtina atkreipti dėmesį ir į tai, kad, nustatytais duomenimis, Ginčijamiems mokėjimams inicijuoti būtini duomenys buvo suvesti suklastotoje interneto svetainėje, kurioje pareiškėjui buvo rodoma informacija, kad už prekę sumokėta, ir buvo prašoma pateikti duomenis, kad lėšos būtų įskaitytos į sąskaitą. Dėl šios priežasties ginčo byloje nėra jokių duomenų, kurie galėtų patvirtinti, kad pareiškėjas, duomenis, būtinus Ginčijamiems mokėjimams inicijuoti, suvedęs suklastotoje interneto svetainėje, turėjo ir galėjo matyti ir tokio tipo operacijas per gavėją inicijavusiems klientams interneto banke įprastai rodomą operacijos aprašymo langą, kuriame ir atvaizduojama pirmiau minėta informacija apie mokėtojo inicijuotą mokėjimą: gavėjas, suma, mokėjimo kortelės paskutiniai 4 skaitmenys ir kontrolinis kodas, kurį reikia sutikrinti su „Smart-ID“ programėlės pranešimo lange matomu kontroliniu kodu.

Vadinasi, ginčo byloje esantys įrodymai, tarp jų ir pirmiau aptarti duomenys dėl Ginčijamų mokėjimų inicijavimo ir įvykdymo aplinkybių, kurių nepaneigė banko paaiškinimai ir pateikti vidinės sistemos duomenys apie tai, kad Ginčijamiems mokėjimams patvirtinti panaudoti pareiškėjo mokėjimo kortelės duomenys ir suvestas pareiškėjo naudojamos „Smart-ID“ paskyros PIN1 kodas, Lietuvos banko vertinimu, leidžia daryti išvadą, kad trečiųjų asmenų sukurtoje aplinkoje pareiškėjui apie inicijuotus Ginčijamus mokėjimus buvo rodoma tikrovės neatitinkanti informacija, kuri galėjo suklaidinti pareiškėją dėl tokių mokėjimo operacijų esmės ir pobūdžio. Vadinasi, duomenų, jog pareiškėjas žinojo, suprato ir išreiškė savo valią autorizuoti Ginčijamus mokėjimus šalių sutarta tvarka ginčo byloje nėra.

Vertinant banko teiginius, kuriais grindžiama jo pozicija dėl Ginčijamų mokėjimų kaip tinkamai autorizuotų, be kita ko, verta atkreipti dėmesį ir į tai, kad ginčo šalių sutartinių santykių neatskiriama dalimi esančiose banko mokėjimo paslaugų teikimo sąlygose ar kituose šalių sutartinius santykius reguliuojančiuose dokumentuose nėra paaiškinama, nurodoma „Smart-ID“, kaip tapatybės patvirtinimo priemonės, PIN kodų suvedimo reikšmė mokėjimo operacijų vykdymo procese ir jų panaudojimo galimos pasekmės klientui, t. y. kokius veiksmus, naudodamasis „Smart-ID“ programėle, banko klientas gali atlikti ir kokie veiksmai bei kokiais atvejais, naudojantis šia tapatybės patvirtinimo priemone ir suvedant jos PIN kodus, sukelia atitinkamas teises pasekmes. Nors „Smart-ID“ ir nėra banko sukurta tapatybės patvirtinimo priemonė, vis dėlto būtent bankas suteikia galimybę naudojantis ja savo klientams (šiuo atveju – pareiškėjui) nuotoliniu būdu patvirtinti savo tapatybę ir išreikšti savo valią atlikti tam tikrus veiksmus, sukeliančius jiems teises pasekmes, t. y. naudotis banko teikiamomis paslaugomis – pateikti mokėjimo nurodymą, pasitikrinti sąskaitą ir pan. Tad banko siūlomos ir (ar) leidžiamos naudoti tapatybės patvirtinimo priemonės ne tik turi būti saugios klientams, kurie su banku susiklosčiusiuose sutartiniuose santykiuose naudoja atitinkamą tapatybės patvirtinimo priemonę, bet ir turi būti aiškios: aiškiai pateiktos jų naudojimo sąlygos ir veiksmų, atliekamų naudojantis „Smart-ID“, teises pasekmės, pavyzdžiui, aiški PIN kodų suvedimo teisinė reikšmė.

Taigi, banko teiginio ir vertinimo, kad pats pareiškėjas išreiškė savo valią ir sutikimą įvykdyti Ginčijamus mokėjimus šalių sutarta forma ir tvarka, nepatvirtina nustatytos aplinkybės. Todėl, remiantis aplinkybe, kad pareiškėjo mokėjimo kortelės duomenys, panaudoti Ginčijamiems mokėjimams inicijuoti, buvo suvesti trečiųjų asmenų sukurtame fiktyviame pašto siuntų bendrovės „Omniva“ interneto puslapyje, sukūrusiame įspūdį, kad pareiškėjo prašoma pateikti duomenis tam, kad lėšos būtų įskaitytos į sąskaitą, galima daryti prielaidą, kad Ginčijami mokėjimai buvo inicijuoti ir patvirtinti ne paties pareiškėjo, o trečiųjų asmenų valiniais veiksmais, nors ir atitiko pareiškėjo ir banko sutartą sutikimo įvykdyti mokėjimo operacijas davimo formą ir tvarką. Lietuvos banko nuomone, vertinti Ginčijaus mokėjimus kaip autorizuotus – atliktus esant paties pareiškėjo sutikimui (kaip tai suprantama Mokėjimų įstatymo 29 straipsnio 1 dalies kontekste), nėra pagrindo, todėl šio ginčo nagrinėjimo metu Lietuvos bankas daro išvadą, kad Ginčijami mokėjimai laikytini neautorizuotais.

Dėl neautorizuotų mokėjimo operacijų pasekmių ir pareiškėjo teisė į Ginčijamų mokėjimų sumos gražinimą

Pagal Mokėjimų įstatymo 38 straipsnio 1 dalį, mokėtojo mokėjimo paslaugų teikėjas privalo gražinti mokėtojui neautorizuotos mokėjimo operacijos sumą ne vėliau kaip iki kitos darbo dienos nuo sužinojimo apie tokios mokėjimo operacijos įvykdymą, išskyrus atvejus, kai mokėtojo mokėjimo paslaugų teikėjas turi pagrįstą priežastį įtarti mokėtojo sukčiavimą ir apie šias priežastis raštu praneša priežiūros institucijai (Lietuvos bankui).

Mokėjimų įstatymo 39 straipsnio 1 dalis nustato, kad mokėtojui gali tekti dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai iki 50 Eur, kai šie nuostoliai patirti dėl: 1) prarastos ar pavogtos mokėjimo priemonės panaudojimo; 2) neteisėto mokėjimo priemonės pasisavinimo. Tačiau, kaip nustatyta Mokėjimų įstatymo 39 straipsnio 2 dalyje, mokėtojas neturi patirti jokių nuostolių, jeigu 1) jis iki mokėjimo operacijos įvykdymo negalėjo pastebėti mokėjimo priemonės praradimo, vagystės arba neteisėto pasisavinimo, išskyrus atvejus, kai jis veikė nesąžiningai; 2) nuostoliai yra patirti dėl mokėjimo paslaugų teikėjo, jo darbuotojo, tarpininko, filialo ar asmenų, kuriems perduotas veiklos funkcijų valdymas, veiksmų ar neveikimo.

Mokėjimų įstatymo 39 straipsnio 3 dalyje nustatyta, kad „mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai, jeigu jis juos patyrė veikdamas nesąžiningai arba tyčia ar dėl didelio neatsargumo neįvykdyęs vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų. Tokiais atvejais šio straipsnio 1 dalyje nustatytas didžiausias nuostolių sumos ribojimas netaikomas.“ Mokėjimų įstatymo 34 straipsnyje reglamentuojamos mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigos: 1) naudotis mokėjimo priemone pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas; 2) sužinojus apie mokėjimo priemonės praradimą, vagystę arba neteisėtą pasisavinimą ar neautorizuotą jos naudojimą, nedelsiant apie tai pranešti mokėjimo paslaugų teikėjui arba jo nurodytam subjektui. Mokėjimo paslaugų vartotojas, gavęs mokėjimo priemonę, privalo imtis veiksmų, kad būtų apsaugoti personalizuoti saugumo duomenys (Mokėjimų įstatymo 34 straipsnio 2 dalis).

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

Įvertinus pirmiau nurodytas Mokėjimų įstatymo nuostatas, galima teigti, kad mokėtojo mokėjimo paslaugų teikėjas gali būti visiškai atleistas nuo pareigos gražinti mokėtojui neautorizuotos mokėjimo operacijos sumą tik tuo atveju, jeigu pateikia įrodymų dėl mokėtojo sukčiavimo (nesąžiningumo arba tyčios) arba didelio neatsargumo (Mokėjimų įstatymo 37 straipsnio 3 dalis ir 39 straipsnio 3 dalis).

Pažymėtina, kad aplinkybių ir duomenų, taip pat ir šalių ginčo dėl to, kad pareiškėjas galėjo veikti nesąžiningai arba tyčia, įskaitant sukčiavimą, nėra. Tai reiškia, kad, siekiant įvertinti, ar bankas pagrįstai atsisako kompensuoti pareiškėjo nuostolius, susijusius su Ginčijamų mokėjimų įvykdymu, ir ar galėtų pareiškėjo atžvilgiu būti taikoma Mokėjimų įstatymo 39 straipsnio 3 dalis, būtina nustatyti, ar pareiškėjo elgesys, atskleidžiant tam tikrus personalizuotus mokėjimo priemonės (banko išduotos mokėjimo kortelės) požymius ir (ar) kiti veiksmai, dėl kurių galėjo būti įvykdyti Ginčijami mokėjimai, vertintini kaip didelis pareiškėjo neatsargumas, dėl kurio visi jo reikalaujami atlyginti nuostoliai turėtų tekti pačiam pareiškėjui.

Antrosios mokėjimo paslaugų direktyvos (toliau – PSD2) preambulės 72 punkte rašoma, kad „siekiant įvertinti galimą mokėjimo paslaugų vartotojo aplaidumą ar didelį aplaidumą, reikėtų atsižvelgti į visas aplinkybes. Įtariamo aplaidumo įrodymai ir laipsnis paprastai turėtų būti vertinami pagal nacionalinę teisę. Tačiau nors aplaidumo sąvoka reiškia, kad pažeidžiamas įsipareigojimas elgtis rūpestingai, didelis aplaidumas turėtų reikšti daugiau nei vien aplaidumą ir apimti labai nerūpestingą elgesį; pavyzdžiui, tai būtų mokėjimo operacijos autorizavimui naudojamų saugumo požymių laikymas prie mokėjimo priemonės atviru ir trečiosioms šalims lengvai atskleidžiamu formatu.“

Didelio neatsargumo sąvoka taip pat plėtojama ir Lietuvos Aukščiausiojo Teismo praktikoje. Kasacinis teismas yra išaiškinęs, kad „didelis neatsargumas kaip kaltės forma pasireiškia neprotingu arba išskirtiniu rūpestingumo nebuvimu, kai asmuo nėra tiek rūpestingas, kiek akivaizdžiai būtina esamomis aplinkybėmis.“²

Lietuvos bankas, nagrinėdamas ginčus dėl nuostolių, susijusių su neautorizuotomis mokėjimo operacijomis, įvykusiomis dėl sukčiavimo atakų, ir spręsdamas dėl mokėjimo paslaugų teikėjo atsakomybės už šių nuostolių atlyginimą, nustačius, kad vartotojas (mokėtojas) jam teisės aktuose ir (ar) sutartyje nustatytas pareigas, susijusias su mokėjimo priemonėmis, vykdė netinkamai, laikosi nuomonės, kad didelis neatsargumas yra vertinamojo pobūdžio aplinkybė. Tai reiškia, kad išvada dėl mokėtojo elgesio vertinimo kaip neatsargaus ar labai neatsargaus dėl neautorizuotos (-ų) mokėjimo operacijos (-ų) darytina kiekvienu konkrečiu atveju, įvertinus ginčo nagrinėjimo metu nustatytų individualių, specifinių aplinkybių visumą, kurią patvirtina ginčo byloje esantys įrodymai ir (arba) yra šalių neginčijamos neautorizuotos mokėjimo operacijos įvykdymo aplinkybės. Taigi, šiuo atveju išvada dėl pareiškėjo, kaip mokėtojo, paprasto ar didelio neatsargumo, kaip vertinamojo pobūdžio aplinkybė, negali būti daroma izoliuotai, išsamiai neįvertinus viso Ginčijamų mokėjimų įvykdymo proceso ir su juo susijusių aplinkybių konteksto.

Nors ir laikosi pozicijos, kad Ginčijami mokėjimai buvo tinkamai autorizuoti, atsiliepime bankas teigia, kad aplinkybė, jog pareiškėjas savo valia atskleidė mokėjimo kortelės duomenis kitiems asmenims, reiškia ir tai, kad jis veikė itin neatsargiai ir neapdairiai ir neapsaugojo savo mokėjimo priemonės personalizuotų saugumo duomenų.

Vertinamų aplinkybių kontekste vis dėlto būtina pažymėti, kad, remiantis pirmiau minėtų Mokėjimų įstatymo nuostatų analize, mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai tik tuo atveju, jei tenkinamos abi sąlygos: mokėtojas ne tik neįvykdo vienos ar kelių jam Mokėjimų įstatyme nustatytų pareigų, bet ir padaro tai elgdamasis nesąžiningai arba tyčia ar būdamas labai neatsargus. Taigi, banko sprendimas nekompensuoti pareiškėjo nuostolių dėl neautorizuotų Ginčijamų mokėjimų įvykdymo galėtų būti vertinamas kaip pagrįstas tik tada, jeigu būtų įrodyta, kad pareiškėjas, atskleisdamas tam tikrus

² Lietuvos Aukščiausiojo Teismo 2017 m. balandžio 13 d. nutartis civilinėje byloje Nr. e3K-3-180-378/2017, 29 punktas.

personalizuotus savo mokėjimo priemonių saugumo duomenis ir taip įgalindamas trečiuosius asmenis inicijuoti ir patvirtinti Ginčijamus mokėjimus, elgėsi itin aplaidžiai – buvo labai neatsargus.

Tad Lietuvos bankas, siekdamas nustatyti, ar pareiškėjo elgesys šiuo atveju gali būti laikomas dideliu neatsargumu, vertino paties pareiškėjo elgesį – pasitikėta pokalbių programėlėje gautame pranešime nurodyta informacija, paspausta joje pateikta nuoroda, suklastotame interneto puslapyje suvesti mokėjimo priemonės personalizuoti saugumo duomenys, taip pat banko veiksmus, kurių jis prevenciškai ėmėsi ir imasi tam, kad supažindintų pareiškėją su sukčiavimo elektroninėje erdvėje rizikomis bei tapatybės patvirtinimo priemonės saugaus naudojimo, jos personalizuotų saugumo žymenų suvedimo ir atskleidimo reikšme bei teisinėmis pasekmėmis.

Vertinant paties pareiškėjo elgesį, svarbu nustatyti, kaip pareiškėjas, kaip mokėjimo paslaugų vartotojas, buvo įtikintas atskleisti savo mokėjimo priemonės personalizuotus saugos duomenis, įgalinčius trečiuosius asmenis inicijuoti Ginčijamus mokėjimus.

Ginčo nagrinėjimo metu buvo nustatyta, kad prieš Ginčijamų mokėjimų įvykdymą pareiškėjas pokalbių programėlėje „WhatsApp“ gavo, kaip pats tuo metu tikėjo, pirkėjo siųstą pranešimą apie „Omniva“ paštomate apmokėtą pareiškėjo parduodamą prekę, paspaudė pranešime pateiktą nuorodą ir suklastotame „Omniva“ puslapyje suvedė prašomus nurodyti duomenis – mokėjimo kortelės turėtojo vardą, pavardę ir kortelės numerį, kurie, kaip paaiškėjo vėliau, buvo nusavinti trečiųjų asmenų (sukčių) ir panaudoti tam, kad būtų inicijuoti Ginčijami mokėjimai. Pareiškėjas teigia, kad, suvedęs banko išduotos mokėjimo kortelės numerį, pastebėjo užrašą „vykdoma mokėjimo operacija“³.

Lietuvos bankas kreipėsi į pareiškėją, prašydamas paaiškinti pirmiau nurodytą teiginį, kad, suvedęs mokėjimo kortelės numerį, pareiškėjas pastebėjo, jog yra „vykdoma mokėjimo operacija“. Pareiškėjas paaiškino, kad paspaudė pokalbių programėlėje „Whatsapp“ nenustatyto asmens, prisistačiusio pirkėju, atsiųstame pranešime pateiktą nuorodą, atsidariusiame interneto puslapyje, pažymėtame kaip „Omniva“ interneto svetainė, suvedė banko išduotos mokėjimo kortelės 16 skaitmenų numerį ir tuomet „aktyvavosi jų programa“ – telefono ekrane atsirado balta banko ikona ir rodyklės, kartojosi užrašas „jungiamasi“. Pareiškėjas nurodo tuomet prisijungęs prie savo interneto banko per stacionarų kompiuterį ir, patikrinęs sąskaitos, susietos su mokėjimo kortele, likutį, pamatė, kad buvo rezervuotos sumos Ginčijamiems mokėjimams įvykdyti.

Vertinant tiek Ginčijamų mokėjimų įvykdymo aplinkybes, tiek pareiškėjo neatsargumo laipsnį, matyti, kad ginčo šalys nesutaria ir skirtingai aiškina, kokie duomenys buvo būtini ir suvesti, taigi, pateikti paslaugos teikėjui (pardavėjui) tam, kad būtų inicijuoti ir patvirtinti Ginčijami mokėjimai. Pareiškėjas teigia ir iš dalies banko atsakomybę už įvykdytus Ginčijamus mokėjimus grindžia teiginiu, kad suklastotoje interneto svetainėje nurodė tik savo vardą, pavardę ir mokėjimo kortelės numerį, to, pareiškėjo teigimu, užteko, kad sukčių naudai būtų įvykdyti Ginčijami mokėjimai. Lietuvos bankui paprašius pareiškėjo pateikti ekrano vaizdus to, ką jis matė suklastotoje interneto svetainėje, suveddamas tariamam lėšų įskaitymui prašomą informaciją, pareiškėjas nurodė, kad tokių duomenų (taigi, duomenų, kurie šiuo atveju pagrįstų pareiškėjo teiginį, kad jo buvo prašoma ir jis atskleidė tik savo vardą, pavardę ir banko išduotos mokėjimo kortelės numerį) pateikti negali.

Kita vertus, siekdamas pagrįsti atsisakymą tenkinti pareiškėjo reikalavimą, kartu su atsiliepimu bankas pateikė duomenis ir juos pagrindžiančius įrodymus, kad Ginčijamiems mokėjimams inicijuoti bei įvykdyti buvo panaudoti ne tik pareiškėjo nurodyti mokėjimo kortelės duomenys, t. y. pareiškėjo vardas, pavardė ir mokėjimo kortelės numeris, bet ir mokėjimo kortelės CVV kodas, o visi Ginčijami mokėjimai buvo patvirtinti ir pareiškėjo naudojamos tapatybės patvirtinimo priemonės „Smart-ID“ paskyros PIN1 kodu, žinomu tik pačiam pareiškėjui. 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 buvimą išlieka, tačiau byloje esančių įrodymų visuma leidžia manyti

³ Kaip minėta, pareiškėjas neigia suvedęs mokėjimo kortelės CVV kodą ar naudojėsis savo tapatybės patvirtinimo priemone - programėle „Smart-ID“ ir (ar) suvedęs jos PIN1 kodą, tuo metu, kai buvo inicijuoti ir patvirtinti Ginčijami mokėjimai.

esant labiau tikėtina atitinkamą faktą buvus, nei jo nebuvus⁴. Nors pareiškėjas neigia, kad Ginčijamiems mokėjimams galėjo būti panaudotas jo mokėjimo kortelės CVV kodas ir kad Ginčijamų mokėjimų įvykdymo metu jis naudojo „Smart-ID“ programėlę bei suvedė jos paskyros PIN1 kodą, banko pateikti banko vidaus sistemos duomenys paneigia šią pareiškėjo poziciją. Kad būtų inicijuoti Ginčijami mokėjimai, ne tik buvo pateikti mokėjimo kortelės duomenys – mokėjimo kortelės turėtojo (t. y. pareiškėjo) vardas ir pavardė, mokėjimo kortelės numeris ir CVV kodas, bet ir kiekvienas Ginčijamas mokėjimas buvo patvirtintas suvedant pareiškėjo „Smart-ID“ paskyros PIN1 kodą⁵. Nesant kitų galimybių ir (ar) ginčo nagrinėjimo metu nenustačius kitokias aplinkybes pagrindžiančių duomenų, kaip Ginčijami mokėjimai galėjo būti inicijuoti ir patvirtinti, pačiam pareiškėjui suvedus tik vardą, pavardę ir mokėjimo kortelės numerį, neginčijant aplinkybės, kad Ginčijami mokėjimai yra neautorizuoti ir jų įvykdyti savo valia pareiškėjas nesiekė, labiau tikėtina, kad būtent pareiškėjas atskleidė duomenis, būtinus Ginčijamiems mokėjimams inicijuoti, o vėliau kiekvieną iš jų patvirtino suveddamas savo naudojamos „Smart-ID“ paskyros PIN1 kodą.

Tobulėjant technologijoms, tobulėja ir sukčiavimo būdai bei priemonės, sudėtingėja pačios sukčiavimo atakos, todėl jas atpažinti ir nuo jų apsaugoti reikia vis didesnio mokėjimo paslaugų vartotojų atidumo ir rūpestingumo. Taigi, dėl naujų sukčiavimo būdų, panaudojant naujas technologijas, atsiradimo būtinas itin didelis vartotojų pastabumas ir apdairumas, kurie kartais dėl sukčiavimo atakos naujumo ir kompleksiskumo peržengia net ir vidutinio vartotojo gebėjimą laiku identifikuoti mėginimą neteisėtu būdu pasisavinti mokėjimo priemonę ir (ar) įvykdyti mokėjimo operacijas, kurių mokėjimo paslaugų vartotojas nesiekia įvykdyti. Dėl šios priežasties manytina, kad mokėjimo paslaugų teikėjai, kaip savo srities profesionalai, turi dėti reikiamas pastangas, kad nuolat kryptingai ir tinkamai informuotų savo klientus (vartotojus) apie sukčiavimo pavojus ir rizikas, susijusias su sukčiavimais elektroninėje erdvėje, ir primintų, kokie ir kaip vartotojų duomenys turėtų būti saugomi ir neatskleisti tretiesiems asmenims.

Vertinant banko veiksmus, kurių jis ėmėsi tam, kad informuotų savo klientus, tarp jų ir pareiškėją, apie el. erdvėje kylančias rizikas, naudojantis mokėjimo paslaugomis, pažymėtina, kad, kaip buvo konstatuota pirmiau, ginčo šalių sutartinių santykių neatskiriamai dalimi esančiose banko mokėjimo paslaugų teikimo sąlygose ar kituose šalių sutartinius santykius reguliuojančiuose dokumentuose nėra paaiškinama tapatybės patvirtinimo priemonės „Smart-ID“, PIN kodų suvedimo reikšmė mokėjimo operacijų vykdymo procese ir jų panaudojimo galimos pasekmės klientui. Taigi, ginčo byloje nėra duomenų, kad pareiškėjas būtų buvęs koku nors būdu tinkamai supažindintas su informacija, kokius veiksmus, naudodamasis „Smart-ID“ programėle, banko klientas gali atlikti, kokie veiksmai ir kokiais atvejais, naudojantis šia tapatybės patvirtinimo priemone ir suvedant jos PIN kodus, sukelia atitinkamas teises pasekmes. Bankas atsiliepė taip pat nenurodė, kaip supažindina klientus, šiuo atveju – pareiškėją, su sukčiavimo elektroninėje erdvėje naudojantis mokėjimo paslaugomis rizikomis.

Kita vertus, neabejotina, kad vartotojai, naudodamiesi mokėjimo paslaugomis elektroninėje erdvėje, taip pat privalo paisyti saugaus elgesio rekomendacijų ir, pagrįstai tikėdamiesi aukštus profesionalumo, rūpestingumo ir atidumo standartus atitinkančio mokėjimo paslaugų teikėjo elgesio, patys būti apdairūs, atidūs ir sąmoningi, nes vartotojų lėšų ir atliekamų mokėjimo operacijų, kaip ir kitų elektroninėje erdvėje teikiamų mokėjimo paslaugų saugumas, priklauso ir nuo tinkamo bei atidaus mokėjimo paslaugų vartotojo pareigų, susijusių su mokėjimo priemonių naudojimu, vykdymo.

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 mokėjimo paslaugų teikimo sąlygų 7.2.5 papunktyje nurodyta, jog klientas įsipareigoja: „laikyti paslapyje visus Kortelės ar Skaitmeninės piniginės, su kuria susieta Kortelė, duomenis (informaciją nurodytą ant kortelės)“, o tų pačių sąlygų 9.2 papunktis įtvirtina kliento, turinčio teisę naudotis mokėjimo priemone, pareigą: „Klientas, gavęs mokėjimo priemonę, privalo imtis veiksmų, kad apsaugotų Personalizuotus saugumo duomenis.“

Taigi, pirmiau aptartos banko mokėjimo paslaugų teikimo sąlygų nuostatos aiškiai ir nedviprasmiškai reglamentuoja, kad už tapatybės priemonės personalizuotų saugumo

⁴ 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.

⁵ Kaip minėta pirmiau, bankas kartu su papildomais paaiškinimais pateikė duomenis, kad galinis įrenginys (pagal jo IP adresą), iš kurio, naudojantis „Smart-ID“ programėle, patvirtinti Ginčijami mokėjimai, yra pareiškėjo įprastai naudojamas galinis įrenginys, jungiantis prie interneto banko.

duomenų konfidencialumą yra atsakingas mokėtojas, šiuo atveju – pareiškėjas. Atsižvelgiant į tai, manytina, kad pareiškėjo elgesys būtų laikomas kaip atitinkantis mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, jei būtų nustatyta, kad pareiškėjas ėmėsi adekvačių veiksmų (arba priešingai – nustačius, kad nuo tam tikrų veiksmų susilaikė) tam, kad jam banko išduotų mokėjimo priemonių personalizuotų saugumo duomenų, įgalinančių inicijuoti ir tvirtinti mokėjimus, konfidencialumas būtų tinkamai užtikrintas, o jam banko išduota mokėjimo priemonė – mokėjimo kortelė, būtų naudojama šalių sutartinius santykius reglamentuojančių dokumentų nustatyta tvarka bei sąlygomis.

Vis dėlto, įvertinus ginčo byloje esančius duomenis ir nustatytas aplinkybes, išvados, kad pareiškėjo elgesys atitiko banko nustatytas naudojimosi mokėjimo priemonėmis sąlygas ir buvo adekvatus, pakankamas tam, kad pareiškėjui nustatytos pareigos, susijusios su mokėjimo priemonių personalizuotų saugumo duomenų konfidencialumo užtikrinimu, būtų tinkamai įvykdytos, daryti nėra galima: nors pareiškėjui į pokalbių programėlę atsiųstas nepažįstamo asmens (tariamo pirkėjo) pranešimas galėjo sukurti pirminį įspūdį, kad šis pranešimas išsiųstas potencialaus pirkėjo, tačiau tai, kad pareiškėjas iki personalizuotų duomenų atskleidimo (pateikimo suklastotoje interneto svetainėje) nesudvejojo pranešime nurodytos informacijos ir jam nepažįstamo siuntėjo patikimumu, leidžia teigti, kad pareiškėjo elgesys Ginčijamų mokėjimų inicijavimo metu nebuvo itin apdairus ir atsargus.

Pareiškėjo kartu su kreipimusi pateiktas ekrano vaizdo įrašas, rodantis interneto svetainę, kurioje pareiškėjas turėjo suvesti nurodytus duomenis, kad patvirtintų tariamą lėšų įskaitymą į banke esančią sąskaitą, taip pat sudaro pirminį įspūdį, kad interneto svetainė yra autentiška, nes naudojamas „Omniva“ prekės ženklas, nurodoma, kad „Gavėjas jau pervedė lėšas“, ir prašoma nurodyti pareiškėjo (kaip nurodoma „siuntėjo“) asmens duomenis, siekiant „Gauti lėšas“, be kita ko, prie dalies „Elemento aprašymas“ pažymima, kad „Aprašymas“ – „vaikiškas elektrinis keturratis“, „Kaina“ - „280 Eur“. Taigi, kaip jau minėta, pagal nuorodą atsidariusiame interneto puslapyje pateikti duomenys ir matomi vaizdai galėjo sukurti pirminį įspūdį, kad pirkėju prisistatęs asmuo iš tiesų siekia įsigyti pareiškėjo siūlomą prekę ir tuo tikslu jau yra atlikęs mokėjimą pareiškėjo naudai. Vis dėlto, vertinant pareiškėjo neatsargumo laipsnį, būtina atsižvelgti į tai, kad pareiškėjui nesukėlė įtarimų aplinkybė, kad yra prašoma nurodyti kortelės numerį, kurį pripažįsta suvedęs, nors pats pareiškėjas siekė gauti lėšų, o ne įvykdyti mokėjimo operacijas. Kaip minėta, pagal banko mokėjimo paslaugų teikimo sąlygas, mokėjimo kortelės personalizuotų saugumo duomenų pateikimas minėtose sąlygose numatytais atvejais laikomas kliento (šiuo atveju – pareiškėjo) sutikimu įvykdyti mokėjimo operaciją, lėšas nurašant iš kliento (šiuo atveju – pareiškėjo) sąskaitos. Pareiškėjui taip pat nesukėlė įtarimų aplinkybė, kad nenustatytas ir, kaip nurodo pareiškėjas, jam nepažįstamas asmuo, siekdamas atsiskaityti už tariamai įsigyjamą prekę, jau yra įvykdęs lėšų pervedimo operaciją pareiškėjo naudai, nors pareiškėjas nurodė, kad nei parduodamos prekės skelbime, nei kitokiu būdu jokių asmens ar jo mokėjimo priemonių personalizuotų saugumo duomenų (pvz., banko sąskaitos numerio, kortelės numerio ir pan.) iki Ginčijamų mokėjimų įvykdymo nėra niekam atskleidęs. Tad atitinkamai ginčo byloje nėra jokių duomenų ir kad pareiškėjas būtų kvestionavęs pagal pranešime paspaustą nuorodą atsidariusio interneto puslapio autentiškumą, o jei tokių abejonių pareiškėjas turėjo, nėra jokių duomenų, kad šias abejones būtų stengęsis išsklaidyti, patikrinti gautos informacijos teisingumą.

Kaip minėta pirmiau, pagal banko mokėjimo paslaugų teikimo sąlygų 6.3.1 papunkčio nuostatas, atsiskaitant kortele, tam tikrais atvejais kortelės turėtojas sutikimą atlikti mokėjimo operaciją taip pat gali patvirtinti, pateikdamas kortelės duomenis. Šalių sutartinius santykius reglamentuojančiuose dokumentuose nėra nurodyta, kad mokėjimo kortelės personalizuotų saugumo duomenų pateikimas gali būti reikalingas ne tik inicijuotoms mokėjimo operacijoms, bet ir lėšų gavimui į su mokėjimo kortele susietą sąskaitą patvirtinti. Vadinasi, pareiškėjas turėjo ir galėjo suprasti, kad mokėjimo kortelės duomenų ir „Smart-ID“ paskyros PIN1 kodo suvedimas yra skirti duoti sutikimą įvykdyti mokėjimo operaciją. Tad toks mokėjimo priemonės personalizuotų saugumo duomenų atskleidimas, turint tikslą patvirtinti lėšų įskaitymą (gavimą) į sąskaitą, šiuo atveju laikytinas ne tik neįprastu, bet ir šalių susitarimo sąlygų neatitinkančiu mokėjimo priemonės (banko pareiškėjui išduotos mokėjimo kortelės) panaudojimu. Manytina, kad pareiškėjas, jeigu tik būtų buvęs pakankamai atidus ir rūpestingas, galėjo pastebėti savo mokėjimo priemonės praradimą, nes pareiškėjui akivaizdžiai turėjo sukelti įtarimų faktas, kad jo buvo prašoma suvesti mokėjimo kortelės personalizuotus saugumo duomenis, kurie būtini mokėjimo operacijai įvykdyti, bet ne lėšoms į su šia mokėjimo kortele susietą sąskaitą gauti, kaip teigia manęs pats pareiškėjas. Lietuvos banko vertinimu, toks pareiškėjo elgesys gali būti

pripažintas kaip elgesys, iš esmės besiskiriantis nuo atsargaus elgesio reikalavimų, tai galiausiai ir lėmė, kad pareiškėjas prarado savo mokėjimo priemonę ir jo vardu trečiųjų asmenų naudai buvo patvirtinti Ginčijami mokėjimai, kurių pats pareiškėjas nesiekė atlikti.

Ginčo byloje esantys įrodymai ir pirmiau analizuotos aplinkybės, susijusios tiek su pačios sukčiavimo atakos pobūdžiu, tiek su banko veiksmais, o svarbiausia – susijusios su paties pareiškėjo veiksmais, vis dėlto nesudaro pagrindo vertinti pareiškėjo elgesio tik kaip neatsargaus. Pareiškėjas ne tik netinkamai vykdė jam, kaip mokėtojui, Mokėjimų įstatyme nustatytas pareigas, susijusias su jam išduotomis mokėjimo priemonėmis ir jų personalizuotais saugumo duomenimis, bet ir darė tai, elgdamasis labai neatsargiai. Tai reiškia, kad pareiškėjo elgesys nebuvo toks, koks akivaizdžiai buvo būtinas, ir tai šiuo atveju lėmė, kad Ginčijami mokėjimai buvo inicijuoti ir įvykdyti trečiųjų asmenų valia ir apgaulingais veiksmais, pačiam pareiškėjui savo valios dėl tokių operacijų neišreiškus.

Konstatavus, kad pareiškėjas, nesilaikydamas jam, kaip mokėtojui, Mokėjimų įstatyme ir sutartyje su banku nustatytų pareigų, susijusių su jam išduotomis mokėjimo priemonėmis, elgėsi labai neatsargiai, kartu darytina išvada, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, nustatančią, kad tokiu atveju mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai. Dėl šios priežasties, Lietuvos banko vertinimu, bankas neturi pareigos gražinti pareiškėjui neautorizuotų Ginčijamų mokėjimų lėšų.

Dėl banko teikiamų mokėjimo paslaugų saugumo

Siekdamas pagrįsti bankui keliamą reikalavimą dėl nuostolių, susijusių su Ginčijamų mokėjimų įvykdymu, kompensavimo, pareiškėjas, be kita ko, teigia, kad aplinkybė, jog Ginčijami mokėjimai buvo įvykdyti, reiškia, kad banko sistemose yra saugumo spragų. Taigi, preziumuotina, kad, pareiškėjo vertinimu, banko pritaikytos ir (ar) taikomos saugumo priemonės (operacijų stebėjimo mechanizmai) yra nepakankamos, o tai patvirtina faktas, kad Ginčijami mokėjimai buvo įvykdyti ir lėšos pervesto sukčių naudai.

2017 m. lapkričio 27 d. Komisijos deleguotojo reglamento (ES) 2018/389, kuriuo Europos Parlamento ir Tarybos direktyva (ES) 2015/2366 papildoma griežto kliento autentiškumo patvirtinimo ir bendrų ir saugių atvirųjų ryšių standartų techniniais reguliavimo standartais (toliau – Reglamentas)⁶, ir kuris priimtas siekiant užtikrinti, kad elektroniniu būdu siūlomoms mokėjimo paslaugoms būtų teikiamos saugiai, įdiegiant technologijas, kuriomis galima užtikrinti saugų vartotojo autentiškumo patvirtinimą ir kuo labiau sumažinti sukčiavimo riziką, 2 straipsnyje nustatyti bendrieji autentiškumo patvirtinimo reikalavimai, kurių tinkamą įvykdymą turi užtikrinti mokėjimo paslaugų teikėjai. Pagal minėto straipsnio nuostatas, mokėjimo paslaugų teikėjai įdiegia operacijų stebėjimo mechanizmus, leidžiančius jiems aptikti neautorizuotas ar nesąžiningas mokėjimo operacijas, kad galėtų įgyvendinti saugumo priemones, nurodytas Reglamento 1 straipsnio a ir b punktuose. Tie mechanizmai yra grindžiami mokėjimo operacijų analize, kurią atliekant atsižvelgiama į mokėjimo paslaugų vartotojui būdingus elementus įprastu būdu naudojant personalizuotus saugumo požymius (1 dalis). Mokėjimo paslaugų teikėjai užtikrina, kad įdiegus operacijų stebėjimo mechanizmus būtų atsižvelgiama bent į kiekvieną iš šių rizika grindžiamų veiksnių: a) neteisėtai sužinotų ar pavogtų autentiškumo nustatymo elementų sąrašus; b) kiekvienos mokėjimo operacijos sumą; c) žinomus sukčiavimo scenarijus teikiant mokėjimo paslaugas; d) užkrėtimo kenkimo programine įranga požymius per bet kurį autentiškumo patvirtinimo procedūros seansą; e) tais atvejais, kai priegos prietaisą arba programinę įrangą suteikė mokėjimo paslaugų teikėjas, mokėjimo paslaugų vartotojui suteikto priegos prietaiso arba programinės įrangos naudojimo ir netinkamo jų naudojimo žurnalą (2 dalis). Be to, remiantis Reglamento nuostatomis, autentiškumo patvirtinimo procedūra turėtų apimti operacijų stebėjimo mechanizmus, kuriais būtų galima nustatyti mėginimus pasinaudoti mokėjimo paslaugų vartotojo personalizuotais saugumo požymiais, kurie buvo prarasti, pavogti arba neteisėtai pasisavinti, ir užtikrinti, kad mokėjimo paslaugų vartotojas, įprastu būdu nurodęs personalizuotus saugumo požymius, būtų teisėtas vartotojas ir kaip toks išreikštų savo sutikimą pervesti lėšas ir gauti informaciją apie savo sąskaitą⁷.

Ginčo nagrinėjimo metu Lietuvos bankas paprašė banko pateikti paaiškinimus dėl pareiškėjo išreikštų abejonių dėl banko taikomų saugumo priemonių ir nurodyti, kaip bankas šiuo atveju vykdė pirmiau aptartus Reglamento reikalavimus, susijusius su mokėjimo operacijų stebėjimo mechanizmų įdiegimu.

⁶ <https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32018R0389&from=EN>

⁷ Reglamento preambulės 1 punktą.

Bankas papildomuose paaiškinimuose Lietuvos bankui nurodo, kad atliekant Ginčijamus mokėjimus buvo suvesti tik pareiškėjui, kaip kortelės turėtojui, žinomi mokėjimo kortelės duomenys - vardas ir pavardė, kortelės numeris, galiojimo data, saugos (CVV) kodas. Bankas pažymi, kad, laikantis Mokėjimų įstatymo ir Reglamento reikalavimų, visų Ginčijamų mokėjimų metu buvo atlikta sugriežtinto autentiškumo patvirtinimo procedūra ir operacijos patvirtintos naudojantis „Smart-ID“ programėle, suvedus jos paskyros PIN1 kodą. Bankas nurodė, kad Reglamento reikalavimai dėl mokėjimo operacijų stebėsenos įdiegimo taikytini tik tada, jeigu mokėjimo kortelės išleidėjas (bankas) nusprendžia netaikyti sugriežtinto autentiškumo patvirtinimo. Todėl, banko nuomone, pareiškėjo ir jo atstovės teiginys apie galimas saugumo spragas banko sistemose nėra pagrįstas, nes buvo įvykdyti visi numatyti saugumo reikalavimai.

Taigi, kaip matyti iš banko pateiktų paaiškinimų, bankas, siekdamas įgyvendinti Reglamento ir Mokėjimų įstatymo reikalavimus, susijusius su saugumo priemonių įgyvendinimu, taiko griežto kliento autentiškumo patvirtinimo saugumo priemones, t. y. bankas klientų inicijuotoms mokėjimo operacijoms autorizuoti taiko saugesnio autentiškumo nustatymo procedūrą, o atitinkamų mokėjimo operacijų stebėseną pagal Reglamente nustatytas sąlygas vykdo tik tada, kai taiko griežto kliento autentiškumo patvirtinimo reikalavimų išimtis.

Lietuvos bankas, atsižvelgdamas į pirmiau minėtas Reglamento 2 straipsnio nuostatas, vis dėlto atkreipia dėmesį, kad pagal šią nuostatą mokėjimo paslaugų teikėjų pareigai įdiegti operacijų stebėjimo mechanizmus, leidžiančius jiems aptikti neautorizuotas ar nesąžiningas mokėjimo operacijas, nėra numatyta taikymo išimčių, t. y. ši pareiga taikoma nepriklausomai nuo to, ar vykdomos mokėjimo operacijos, kurioms būtina griežta kliento autentiškumo patvirtinimo procedūra, ar tai mokėjimo operacijos, kurioms galioja griežto kliento autentiškumo patvirtinimo reikalavimų išimtis. Todėl, Lietuvos banko nuomone, Reglamento 2 straipsnio nuostatos turėtų būti vertinamos kaip apimančios mokėjimo paslaugų teikėjų pareigą įdiegti mokėjimo operacijų stebėjimo mechanizmus tiek tada, kai galioja griežto kliento autentiškumo patvirtinimo reikalavimų išimtis, tiek tada, kai būtina taikyti griežtą kliento autentiškumo patvirtinimo procedūrą.

Kaip minėta, nagrinėdamas ginčą Lietuvos bankas neatlieka patikrinimų tam, kad nustatytų, ar nebuvo pažeisti teisės aktų reikalavimai. Lietuvos bankas remiasi ginčo šalių pateiktais konkrečiais įrodymais, kurių pagrindu priima sprendimą. Įvertinus konstatuotas aplinkybes, vis dėlto matyti, kad ginčo byloje nėra duomenų, galinčių patvirtinti aplinkybę, kad bankas, įvykdydamas Ginčijamus mokėjimus, būtų pažeidęs finansų rinką reglamentuojančių teisės aktų reikalavimus. Taigi, nors pareiškėjas kreipimesi teigia, kad banko sistemose yra saugumo spragų, tačiau jokių savo teiginį patvirtinančių įrodymų nepateikė, t. y. plačiau nepaaiškino ir nepagrindė, kokie banko įdiegtų (mokėjimo) sistemų trūkumai, net ir pareiškėjui elgiantis itin apdairiai su išduotomis mokėjimo priemonėmis ir jų personalizuotais saugumo duomenimis, galėjo nulemti Ginčijamų mokėjimų įvykdymą ir dėl to galėtų kilti atitinkama banko civilinė atsakomybė šių mokėjimų nulemtus nuostolius pareiškėjui kompensuoti. Pažymėtina, kad vien aplinkybė, jog Ginčijami mokėjimai buvo įvykdyti, kaip pareiškėjas nurodo, sukčių naudai, savaime nepagrindžia aplinkybės, kad banko taikytos saugumo priemonės šiuo konkrečiu atveju buvo ne tik nepakankamos, bet ir neatitinkančios teisės aktų reikalavimų.

Dėl mokėjimo nurodymo neatšaukiamumo

Vertinant pareiškėjo, kaip mokėtojo, galimybę atšaukti mokėjimo nurodymus įvykdyti Ginčijamus mokėjimus, papildomai pažymėtina, kad, 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. Minėto Mokėjimų įstatymo straipsnio 4 dalyje taip pat nustatyta, kad, pasibaigus 1 dalyje nurodytam laikotarpiui, mokėjimo nurodymas gali būti atšauktas tik tuo atveju, kai dėl to susitaria mokėjimo paslaugų vartotojas ir atitinkamas mokėjimo paslaugų teikėjas, o šio straipsnio 2 dalyje numatytais atvejais būtinas ir gavėjo sutikimas. Mokėjimo paslaugų teikėjas gali imti komisinį atlyginimą už mokėjimo nurodymo atšaukimą, jeigu tai numatyta bendrojoje sutartyje. Taigi, pasibaigus Mokėjimų įstatymo 44 straipsnio 1 dalyje nurodytam terminui, mokėjimo nurodymas gali būti atšauktas tik dėl to susitarus vartotojui ir jo mokėjimo paslaugų teikėjui, todėl nurodytos galimybės (t. y. mokėjimo nurodymo atšaukimo) įtvirtinimas Mokėjimų įstatyme neturėtų būti vertinamas kaip priverstinis lėšų gražinimas mokėtojui, esant jo atitinkamam prašymui (pasibaigus 44 straipsnio 1 dalyje nurodytam terminui).

Banko mokėjimo paslaugų teikimo sąlygų 6.3.3 papunktyje nurodyta, kad mokėjimo nurodymas negali būti atšauktas po to, kai jį iš mokėtojo gauna bankas, išskyrus šiose sąlygose nustatytais atvejais. Tais atvejais, kai mokėjimo operacija inicijuojama mokėjimo inicijavimo paslaugos teikėjo arba gavėjo ar per gavėją, klientas negali atšaukti mokėjimo nurodymo po to, kai mokėjimo inicijavimo paslaugos teikėjui davė sutikimą inicijuoti mokėjimo operaciją arba gavėjui davė sutikimą atlikti mokėjimo operaciją. Klientas, davęs mokėjimo inicijavimo paslaugos teikėjui sutikimą inicijuoti mokėjimo operaciją yra atsakingas už sutikimo davimą ir negali atšaukti mokėjimo nurodymo po to, kai davė sutikimą inicijuoti mokėjimo operaciją (6.3.4 papunktis). Mokėjimo nurodymai, nustatyti sąlygų 6.4.2 papunktyje (t. y. kai susitariama juos įvykdyti konkrečią datą ar konkrečiu laikotarpiu), gali būti atšaukti ne vėliau kaip iki darbo dienos, einančios prieš sutartą dieną, pabaigos (6.3.5 papunktis). Pasibaigus banko mokėjimo paslaugų teikimo sąlygų 6.3.3 ir 6.3.5 punktuose nustatytiems terminams, mokėjimo nurodymas gali būti atšauktas tik kliento ir banko susitarimu (6.3.6 papunktis).

Pažymėtina, kad nei Mokėjimų įstatyme, nei šalių susitarime (banko mokėjimo paslaugų teikimo sąlygose) nurodytos sąlygos atšaukti mokėjimo nurodymą įvykdyti Ginčijamus mokėjimus nagrinėjamo ginčo atveju nebuvo nustatytos, t. y. pareiškėjas į banką su prašymu atšaukti mokėjimo nurodymus įvykdyti Ginčijamus mokėjimus paskambino po to, kai sutikimai įvykdyti minėtas mokėjimo operacijas jau buvo duoti ir banko mokėjimo paslaugų teikimo sąlygose nurodytas terminas atšaukti mokėjimo nurodymus jau buvo praėjęs.

Kreipimesi pareiškėjo atstovė papildomai nurodo, kad rezervuotos Ginčijamų mokėjimų lėšų iš su mokėjimo kortele susietos pareiškėjo sąskaitos banke buvo nurašytos ir pervestos į sukčių sąskaitą nepaisant to, kad pareiškėjas prieš tai buvo skambinęs į banką, prašydamas jo mokėjimo priemones užblokuoti ir Ginčijamus mokėjimus atšaukti. Atsižvelgdamas į tai, bankas atsiliepime paaiškina, kad mokėjimo kortelių operacijų patvirtinimo užklausas bankas gauna ir vykdo pagal tarptautinės mokėjimo kortelių organizacijos „Visa“ nustatytas taisykles: gavęs užklausą rezervuoti lėšas, jas rezervuoja mokėjimo kortelės sąskaitoje, o šias lėšas nurašo, tik gavęs paslaugos ar prekės tiekėjo banko patvirtinimą. Nurodytų aplinkybių kontekste pažymėtina, kad nurodytus banko teiginius patvirtina banko mokėjimo paslaugų teikimo sąlygų 7.2.24 papunkčio nuostatos, pagal kurias bankas, gavęs kliento (kortelės turėtojo) sutikimą atsiskaityti kortele, su ja susietoje mokėjimo sąskaitoje rezervuoja operacijos lėšas ir, gavęs iš lėšų gavėjo duomenis ir patvirtinimą apie atsiskaitymus kortele, jas nurašo. Remdamasis minėtomis mokėjimo paslaugų teikimo sąlygų nuostatomis, bankas panaikina lėšų rezervaciją su kortele susietoje sąskaitoje, jei per 9 kalendorines dienas nuo lėšų rezervavimo datos iš lėšų gavėjo negauna duomenų ir patvirtinimo apie atsiskaitymą kortele.

Ginčo nagrinėjimo metu nustatytais duomenimis, gautos užklauskos rezervuoti lėšas pareiškėjo su mokėjimo kortele susietoje sąskaitoje buvo pateiktos pagal tarptautinės mokėjimo kortelių organizacijos „Visa“ nustatytas taisykles, t. y. buvo suvesti mokėjimo kortelės duomenys – pareiškėjo (mokėjimo kortelės turėtojo) vardas ir pavardė, kortelės numeris (tą patvirtina ir pareiškėjas savo kreipimesi). Taip pat, banko pateiktais duomenimis, Ginčijamų mokėjimų inicijavimo metu buvo suvestas mokėjimo kortelės CVV kodas ir Ginčijami mokėjimai papildomai patvirtinti, identifikuojant kortelės turėtoją jo pasirinktu autentifikavimo metodu – suvedus pareiškėjo naudojamos „Smart-ID“ paskyros PIN1 kodą. Dėl šios priežasties manytina, kad lėšos Ginčijamiems mokėjimams įvykdyti pareiškėjo su mokėjimo kortele susietoje sąskaitoje buvo rezervuotos pagrįstai, o praėjus teisės aktuose ir šalių susitarimo sąlygose nustatytiems terminams mokėjimo nurodymus atšaukti, bankas neturėjo pareigos, o šiuo atveju ir galimybės pareiškėjo vardu pateiktų mokėjimo nurodymų įvykdyti Ginčijamus mokėjimus atšaukti.

Todėl, įvertinus visa tai, kas išdėstyta pirmiau, ir ypač atsižvelgiant į tai, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, darytina išvada, kad pareiškėjo bankui keliamas reikalavimas grąžinti pareiškėjui įvykdytų Ginčijamų mokėjimų lėšas yra nepagrįstas, todėl atmestinas.

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

Atmesti 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. Ginčo šalys turi pareigą pranešti Lietuvos bankui, jeigu viena iš ginčo šalių pareiškia ieškinį bendrosios kompetencijos teismui prašydama nagrinėti tapatų ginčą iš esmės.

[Pareigų pavadinimas]

[Vardas ir pavardė]