# LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

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

2023-12-06 Nr. 429-530
Vilnius

Lietuvos bankas gavo X. X. (toliau – pareiškėja) kreipimąsi, kuriuo prašoma išnagrinėti tarp pareiškėjos ir *Luminor Bank AS*, veikiančio per skyrių Lietuvoje, (toliau – bankas) kilusį ginčą.

N u s t a t y t a:

2023 m. liepos 15 d., panaudojant banko išduotos pareiškėjos mokėjimo kortelės „Visa" duomenis, buvo atliktos dvi mokėjimo operacijos, kurių suma 3 751,13 Eur, lėšų gavėjams *Monobank Kyiv UA* ir *Mercuryo Mercuryo LT* (toliau – Operacijos).

Tą pačią dieną pareiškėja telefonu kreipėsi į banką ir pranešė, kad socialiniame tinkle „Facebook" paskelbė skelbimą apie jos pačios parduodamą prekę. Pareiškėja nurodė, kad dėl prekės į ją kreipėsi tretieji asmenys. Pareiškėja per mobiliąją pokalbių programėlę „Messenger" gavo nepažįstamo pirkėju prisistačiusio asmens žinutę, kad šis asmuo siekia įsigyti parduodamą prekę pagal pareiškėjos įkeltą skelbimą. Pareiškėjos teigimu, pirkėju prisistatęs asmuo jai vėliau atsiuntė ir nuorodą į siuntų pristatymo bendrovės „Omniva" interneto svetainę, kurioje pareiškėja turėjo suvesti savo mokėjimo kortelės duomenis tam, kad tariamo pirkėjo pervesta suma už pareiškėjos parduodamą prekę būtų įskaityta į pareiškėjos sąskaitą banke. Pareiškėja vykdė trečiojo asmens nurodymus ir suvedė savo mokėjimo kortelės duomenis minėtoje interneto svetainėje, o Operacijas papildomai patvirtino „Smart-ID" programėlės PIN1 kodu.

Pokalbio metu pareiškėjos mokėjimo kortelė buvo užblokuota ir pareiškėjai rekomenduota prisijungus prie interneto banko paskyros užpildyti prašymą dėl galimybės susigrąžinti Operacijų metu pervestas lėšas.

2023 m. liepos 15 d. pareiškėja užpildė prašymą įvertinti Operacijas ir grąžinti pareiškėjos prarastas lėšas.

Remdamasis visa surinkta informacija, bankas priėmė sprendimą atsisakyti pareiškėjai atlyginti jos patirtus nuostolius, nes nustatė, kad pati pareiškėja perdavė mokėjimo kortelės duomenis tretiesiems asmenims ir davė sutikimą atlikti Operacijas. Dėl šios priežasties bankas nurodė, kad būtent pareiškėja elgėsi labai neatsargiai, todėl ji yra atsakinga už jos patirtus nuostolius. Pareiškėja su tuo nesutiko, todėl tarp šalių kilo ginčas.

Kreipimesi į Lietuvos banką pareiškėja prašo banko grąžinti Operacijų metu iš pareiškėjos atsiskaitomosios sąskaitos nurašytas lėšas, t. y. grąžinti 3 751,13 Eur. Pareiškėja Lietuvos bankui nurodė analogiškas aplinkybes kaip ir kreipimesi į banką. Pareiškėja papildomai nurodė, kad jai pasirodžiusiuose „Smart-ID" pranešimuose papildomai nebuvo rodoma jokia informacija, dėl kokios priežasties ji turėjo suvesti „Smart-ID" PIN1 kodą. Pareiškėja teigia laukusi, kol reikės suvesti „Smart-ID" PIN2 kodą, tačiau šio etapo nereikėjo, o Operacijos jau buvo atliktos. Pareiškėja nurodo dėl šios priežasties nepastebėjusi, kad sukčiai atliko Operacijas ir ji prarado lėšas. Pareiškėjos teigimu, daugėjant sukčiavimo atakų, bankas turi sukurti apsaugos mechanizmą, kad pats vartotojas, iškilus neaiškumų, galėtų valdyti mokėjimo operacijos nepatvirtinimo arba atšaukimo procesą ir taip apsaugoti savo lėšas.

Atsiliepime į pareiškėjos kreipimąsi bankas nurodo nesutinkąs su pareiškėjos reikalavimu ir prašo jį atmesti. Banko teigimu, pareiškėja dėl savo didelio neatsargumo neišsaugojo savo personalizuotų saugos duomenų, dėl to tretieji asmenys jais galėjo pasinaudoti ir be pareiškėjos žinios inicijuoti Operacijas. Bankas nurodo, kad norint gauti lėšas į savo sąskaitą nereikia suvesti savo mokėjimo kortelės duomenų bei patvirtinti savo tapatybės.

Papildomai bankas pažymėjo, kad Operacijos buvo įvykdytos jas patvirtinus saugesnio autentiškumo patvirtinimo procedūra – buvo suvesti tik pareiškėjai žinomi jos mokėjimo kortelės duomenys (vardas, pavardė, kortelės numeris, galiojimo data ir saugos kodas (CVV)), o Operacijos patvirtintos suvedus pareiškėjos naudojamos tapatybės atpažinties priemonės „Smart-ID" paskyros PIN1 kodą. Bankas atkreipia dėmesį į tai, kad pati pareiškėja neginčija fakto, kad perdavė tretiesiems asmenims mokėjimo kortelės duomenis ir pati suvedė turimame mobiliajame telefone tik jai vienai žinomą „Smart-ID" PIN1 kodą. Bankas nurodė, kad kai mokėtojas suveda mokėjimo kortelės duomenis ir identifikacijai pasirenka „Smart-ID", kortelės turėtojas, t. y. banko klientas, nustatomas tik pagal PIN1 kodą, o PIN2 kodas nėra vedamas. Banko teigimu, pareiškėjos elgesys turi būti laikomas kaip neatitinkantis mokėjimo priemonės išdavimą ir naudojimą reglamentuojančių sąlygų, nes pareiškėja nesutikrino „Smart-ID" programėlės kontrolinio saugos kodo, suvedė tik jai žinomą slaptažodį, o tai ir lėmė, kad pareiškėjos vardu buvo duotas sutikimas atlikti Operacijas.

Bankas teigia ir tai, kad, rūpindamasis lėšų saugumu, periodiškai informuoja savo klientus, įskaitant ir pareiškėją, bei primena, kokios yra saugaus naudojimosi banko teikiamomis el. paslaugomis rekomendacijos. Atsižvelgdamas į visas pirmiau nurodytas aplinkybes, bankas prašė atmesti pareiškėjos 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 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. Nagrinėdamas ginčą Lietuvos bankas atlieka ginčo šalių pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Pareiškėjos ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjai Operacijų metu iš jos atsiskaitomosios sąskaitos banke pervestą sumą. Pareiškėja neigia autorizavusi Operacijas, todėl mano, kad bankas Operacijų lėšas turi grąžinti pareiškėjai. Banko vertinimu, pareiškėjos veiksmams būdingas didelis neatsargumas, todėl bankas negali būti įpareigotas Operacijų sumos grąžinti pareiškėjai.

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

Mokėjimų įstatymo 29 straipsnio 1 dalyje nustatyta, kad mokėjimo operacija laikoma autorizuota tik tada, kai mokėtojas duoda sutikimą įvykdyti mokėjimo operaciją. Jeigu mokėtojo sutikimo įvykdyti mokėjimo operaciją nėra, laikoma, kad mokėjimo operacija yra neautorizuota (Mokėjimų įstatymo 29 straipsnio 2 dalis).

Pareiškėjos nurodytos aplinkybės, kad Operacijos nėra pareiškėjos autorizuotos, o pareiškėjos personalizuotus saugumo duomenis ir pareiškėjos sutikimą tretieji asmenys gavo apgaulės būdu, bankas atsiliepime neginčija. Priešingai, bankas savo paaiškinimuose nurodo, kad dėl pareiškėjos atskleistų duomenų tretieji asmenys įgijo galimybę inicijuoti Operacijas. Dėl šios priežasties yra akivaizdu, kad Operacijų inicijavimas ir patvirtinimas neatitiko pačios pareiškėjos valios, nors formaliai (pagal išorinius požymius) ir sutapo su pareiškėjos ir banko sutarta sutikimo atlikti mokėjimo operacijas davimo forma ir tvarka. Atsižvelgdamas į tai, Lietuvos bankas daro išvadą, kad Operacijos, atliktos nesant pareiškėjos valios ir jai net nežinant apie Operacijų inicijavimo aplinkybę bei neišreiškus jokių valinių veiksmų patvirtinti Operacijas, laikytinos neautorizuotomis.

*Siekdamas išspręsti tarp šalių kilusį ginčą ir įvertinti pareiškėjos bankui keliamo reikalavimo pagrįstumą, Lietuvos bankas vertins, ar bankas, atsisakydamas grąžinti pareiškėjai Operacijų metu pervestas lėšas, pagrįstai rėmėsi Mokėjimų įstatymo 39 straipsnio 3 dalimi.*

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 neįvykdęs vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų.

Taip pat svarbu pažymėti, kad Lietuvos Aukščiausiasis Teismas yra konstatavęs, kad įstatyme nustatyta tokia mokėtojo paslaugų teikėjo atsakomybės už neautorizuotą mokėjimą sistema, pagal kurią mokėtojas turi teisę į neautorizuotos operacijos sumos sugrąžinimą, o mokėtojo paslaugos teikėjas turi pareigą ją sugrąžinti, išskyrus atvejus, jei nustatoma, kad: 1) mokėtojas veikia nesąžiningai; 2) mokėtojas tyčia ar dėl didelio neatsargumo pažeidžia vieną ar kelias Mokėjimų įstatymo 34 straipsnyje nustatytas mokėtojo pareigas, susijusias su mokėjimo priemonėmis ir personalizuotais saugumo duomenimis. Nurodyta mokėtojo paslaugų teikėjo atsakomybės už neautorizuotą mokėjimą sistema reiškia griežtąją mokėtojo paslaugų teikėjo atsakomybę už atliktas neautorizuotas mokėjimo operacijas, t. y. atsakomybę be kaltės. Kita vertus, mokėtojo paslaugų teikėjo atsakomybė be kaltės neeliminuoja paties mokėtojo pareigos elgtis rūpestingai ir atsakingai. Jeigu mokėtojas elgiasi nesąžiningai ar tyčia ar dėl didelio neatsargumo pažeidžia įstatyme jam nustatytas pareigas, paslaugos teikėjas yra atleidžiamas nuo atsakomybės. Ne bet kokių mokėtojo pareigų nevykdymas yra pagrindas atleisti mokėtojo paslaugos teikėją nuo atsakomybės, o būtent Mokėjimų įstatymo 34 straipsnyje nustatytų mokėtojo pareigų, kurios susijusios su mokėjimo priemonėmis ir personalizuotais saugumo duomenimis, be to, paprastas mokėtojo neatsargumas nėra laikomas mokėtojo paslaugos teikėjo atleidimo nuo atsakomybės sąlyga[1].

Duomenų, kad nagrinėjamu atveju pareiškėja galėjo veikti nesąžiningai arba tyčia, nėra, todėl galimas mokėtojo sukčiavimas, kaip pagrindas atleisti mokėtojo mokėjimo paslaugų teikėją nuo pareigos atlyginti mokėtojui nuostolius dėl neautorizuotos mokėjimo operacijos įvykdymo, šiame sprendime atskirai nebus plačiau analizuojamas.

Taigi, sprendžiant, ar banko atsisakymas grąžinti pareiškėjai Operacijų sumą laikytinas pagrįstu, būtina įvertinti, ar pareiškėjos elgesys, atskleidžiant tretiesiems asmenims personalizuotus saugumo duomenis, vertintinas kaip didelis neatsargumas, dėl kurio su mokėjimo operacijos įvykdymu atsiradę nuostoliai, kaip nustatyta Mokėjimų įstatymo 39 straipsnio 3 dalyje, tektų pačiai pareiškėjai.

Lietuvos Aukščiausiasis Teismas yra išaiškinęs, kad didelis neatsargumas pasireiškia neprotingu arba išskirtiniu rūpestingumo nebuvimu, kai asmuo nėra tiek rūpestingas, kiek akivaizdžiai būtina esamomis aplinkybėmis[2]. Didelis mokėtojo neatsargumas gali būti konstatuojamas tik tuomet, jei mokėtojas elgėsi labai nerūpestingai. Kad mokėtojas elgėsi labai nerūpestingai, turi įrodyti mokėjimo paslaugų teikėjas, pateikdamas konkrečius tokį elgesį pagrindžiančius įrodymus. Ši įrodinėjimo našta negali būti perkelta mokėtojui[3].

Dėl mokėtojo neatsargumo laipsnio vertinimo, pagrindinių jo kriterijų ir glaudaus ryšio su ginčo byloje nustatytų individualių specifinių aplinkybių visuma Lietuvos bankas yra ne kartą plačiau pasisakęs savo ginčų nagrinėjimo praktikoje[4], todėl šiame sprendime bus pasisakoma tik šiai konkrečiai ginčo bylai aktualiais aspektais.

Neautorizuotos mokėjimo operacijos įvykdymo atveju didelis neatsargumas yra sietinas su vienos ar kelių Mokėjimų įstatymo 34 straipsnyje mokėtojui nustatytų pareigų, susijusių su mokėjimo priemone ir personalizuotais saugumo duomenimis, nevykdymu. Kaip yra konstatavęs Lietuvos Aukščiausiasis Teismas, neautorizuotos mokėjimo operacijos atveju mokėjimo paslaugų teikėjas turi įrodyti ne tik tai, kad mokėtojas pažeidė vieną ar kelias Mokėjimų įstatymo 34 straipsnyje nustatytas mokėtojo pareigas, susijusias su mokėjimo priemonėmis ir personalizuotais saugumo duomenimis, bet ir kad tai padarė dėl didelio neatsargumo[5].

Mokėjimų įstatymo 34 straipsnis nustato mokėtojo pareigą naudotis jam išduota mokėjimo priemone (nagrinėjamu atveju – mokėjimo kortele) pagal jos išdavimą ir naudojimą reglamentuojančias sąlygas, o sužinojus apie jos praradimą, vagystę arba neteisėtą pasisavinimą ar neautorizuotą jos naudojimą, nedelsiant apie tai pranešti mokėjimo paslaugų teikėjui arba jo nurodytam subjektui (Mokėjimų įstatymo 34 straipsnio 1 dalis), taip pat pareigą, gavus mokėjimo priemonę, imtis veiksmų, kad būtų apsaugoti personalizuoti saugumo duomenys (Mokėjimų įstatymo 34 straipsnio 2 dalis).

Bankas mano, kad nuostolius dėl Operacijų pareiškėja patyrė dėl savo didelio neatsargumo, t. y. pareiškėja, perduodama tretiesiems asmenims savo mokėjimo kortelės duomenis (mokėjimo kortelėje nurodytus savo vardą, pavardę, kortelės numerį ir CVV kodą) ir

---

[1] Lietuvos Aukščiausiojo Teismo 2023 m. rugsėjo 12 d. nutartis civilinėje byloje Nr. e3K-3-182-1075/2023, 44 punktas.
[2] Lietuvos Aukščiausiojo Teismo 2017 m. balandžio 13 d. nutartis civilinėje byloje Nr. e3K-3-180-378/2017.
[3] Lietuvos Aukščiausiojo Teismo 2023 m. rugsėjo 12 d. nutartis civilinėje byloje Nr. e3K-3-182-1075/2023, 82 punktas.
[4] Pavyzdžiui, ginčo bylos Nr. 2022-00586 ir 2022-02496.
[5] Lietuvos Aukščiausiojo Teismo 2023 m. rugsėjo 12 d. nutartis civilinėje byloje Nr. e3K-3-182-1075/2023, 78 punktas.

patvirtindama Operacijas suvesdama tik jai žinomą „Smart-ID" programėlės PIN1 kodą, suteikė leidimą tretiesiems asmenims mokėjimo kortele inicijuoti ir atlikti Operacijas pareiškėjos vardu.

Vertinamų aplinkybių kontekste visų pirma 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, t. y. mokėtojas ne tik neįvykdo vienos ar kelių jam Mokėjimų įstatyme nustatytų pareigų, bet ir padaro tai elgdamasis nesąžiningai arba tyčia, arba būdamas labai neatsargus. Taigi, banko sprendimas nekompensuoti pareiškėjos nuostolių dėl neautorizuotų Operacijų įvykdymo galėtų būti vertinamas kaip pagrįstas tik tada, jeigu būtų įrodyta, kad pareiškėja, atskleisdama tam tikrus personalizuotus savo mokėjimo priemonių saugumo duomenis, leido inicijuoti ir net patvirtino Operacijas, t. y. elgėsi itin aplaidžiai – buvo labai neatsargi.

Lietuvos bankas, siekdamas nustatyti, ar pareiškėjos elgesys šiuo atveju gali būti laikomas dideliu neatsargumu, vertino pareiškėjos elgesį pasitikint pokalbių programėlėje gautame pranešime nurodyta informacija ir spaudžiant joje pateiktą nuorodą, suvedant savo mokėjimo priemonės personalizuotus saugumo duomenis suklastotame interneto puslapyje bei patvirtinant atliekamus veiksmus (savo tapatybę) naudojama atpažinties priemone – suvedant „Smart-ID" programėlės PIN1 kodą, 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 pačios pareiškėjos elgesį, svarbu nustatyti, kaip pareiškėja, kaip mokėjimo paslaugų vartotoja, buvo įtikinta atskleisti savo mokėjimo priemonės personalizuotus saugos duomenis, įgalinusius trečiuosius asmenis inicijuoti Operacijas.

Lietuvos bankas, įvertinęs pareiškėjos kreipimesi ir banko atsiliepime nurodytas aplinkybes bei kartu su kreipimusi ir atsiliepimu pateiktus duomenis, nustatė, kad prieš Operacijų įvykdymą pareiškėja pokalbių programėlėje „Messenger" gavo, kaip pati tuo metu tikėjo, pirkėjo siųstą pranešimą apie siuntų bendrovės „Omniva" sistemoje apmokėtą pareiškėjos parduodamą prekę, paspaudė pranešime pateiktą nuorodą ir suklastotame „Omniva" puslapyje suvedė prašomus nurodyti duomenis: mokėjimo kortelės turėtojo vardą, pavardę ir kortelės numerį ir CVV kodą, kurie, kaip paaiškėjo vėliau, buvo nusavinti trečiųjų asmenų (sukčių) ir panaudoti tam, kad būtų inicijuotos Operacijos.

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. *Luminor* mokėjimo paslaugų teikimo sąlygų[6] (toliau – Sąlygos) 3.1 papunkčio 26 dalyje yra įtvirtintas mokėjimo kortelės apibrėžimas: „mokėjimo kortelė – tai Banko Klientui suteikta elektroninė mokėjimo priemonė, leidžianti Klientui elektroniniu būdu suformuoti mokėjimo nurodymus Bankui dėl disponavimo su kortele susietoje mokėjimo sąskaitoje esančiomis Kliento lėšomis, t. y. atsiskaityti už prekes ir paslaugas negrynaisiais pinigais prekybos ir paslaugų įmonėse jų darbo metu, išsiimti bei įnešti grynuosius pinigus jų išdavimo / priėmimo vietose ir automatuose jų darbo metu. Sąlygose vartojama „kortelės" sąvoka apima tiek papildomą kortelę, tiek pagrindinę kortelę. Pagrindine laikoma kortelė, kuri yra išduota Kliento vardu, o papildoma kortele laikoma kortelė, kuri yra išduota papildomai prie pagrindinės kortelės Kliento ar jo nurodyto asmens vardu."

Sąlygų 7.2.5 papunktyje pareiškėjai, kaip mokėjimo priemonės naudotojai, yra nustatytos pareigos – „laikyti paslaptyje visus Kortelės ar Skaitmeninės piniginės, su kuria susieta Kortelė, duomenis (informaciją nurodytą ant kortelės), įskaitant ir SMS žinute atsiųstą saugos kodą". Sąlygų 9.2 papunktyje yra nustatyta, kad „Klientas, gavęs mokėjimo priemonę, privalo imtis veiksmų, kad apsaugotų Personalizuotus saugumo duomenis". Taip pat Sąlygų 6.3.1 papunktyje, nurodančiame, kokiais būdais banko klientas gali pateikti sutikimą atlikti operaciją, yra nustatyta, kad „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 priemones 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 priglaudimas prie specialiu ženklu pažymėto kortelių aptarnavimo skaitytuvo,

[6] Pareiškėja su šiomis sąlygomis buvo supažindinta 2022 m. rugpjūčio 25 d. laišku interneto banke, kurį pareiškėja perskaitė 2022 m. rugpjūčio 31 d.

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."

Taigi, pirmiau aptartos mokėjimo kortelės sutarties (ją sudarančių dokumentų) nuostatos aiškiai nustato, kad už mokėjimo ir tapatybės patvirtinimo priemonių personalizuotų saugumo duomenų konfidencialumą yra atsakingas mokėtojas, šiuo atveju – pareiškėja, ji privalo užtikrinti, kad minėti duomenys netaptų žinomi tretiesiems asmenims. Atsižvelgiant į tai, manytina, kad pareiškėjos elgesys būtų laikomas kaip atitinkantis mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, jei būtų nustatyta, kad pareiškėja ėmėsi adekvačių veiksmų (arba priešingai – nustačius, kad nuo tam tikrų veiksmų susilaikė) tam, kad jai banko išduotų mokėjimo priemonių personalizuotų saugumo duomenų, įgalinančių inicijuoti ir tvirtinti mokėjimus, konfidencialumas būtų tinkamai užtikrintas, o jai 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 ginčo nagrinėjimo metu nustatytas aplinkybes, išvados, kad pareiškėjos elgesys atitiko banko nustatytas naudojimosi mokėjimo priemonėmis sąlygas ir buvo adekvatus, pakankamas tam, kad pareiškėjai nustatytos pareigos, susijusios su mokėjimo priemonių personalizuotų saugumo duomenų konfidencialumo užtikrinimu, būtų tinkamai įvykdytos, daryti negalima.

Nors pareiškėjai į pokalbių programėlę atsiųstas nepažįstamo asmens (tariamo pirkėjo) pranešimas galėjo sukurti pirminį įspūdį, kad šis pranešimas išsiųstas potencialaus pirkėjo, tačiau tai, kad pareiškėja iki personalizuotų duomenų atskleidimo (pateikimo suklastotoje interneto svetainėje) nesudvejojo pranešime nurodytos informacijos ir jai nepažįstamo siuntėjo patikimumu, leidžia teigti, kad pareiškėjos elgesys, suteikiant tretiesiems asmenims personalizuotus saugumo duomenis, tai turėjo įtakos, kad tretieji asmenys turėjo galimybę inicijuoti Operacijas, nebuvo itin apdairus ir atsargus.

Svarbu pažymėti, kad trečiųjų asmenų pareiškėjai atsiųsta nuoroda https://omniva.lt-info.siuntu-pervezimas.com/cash58714190 skyrėsi nuo tikros bendrovės „Omniva" interneto svetainės nuorodos (tikra svetainės nuoroda https://www.omniva.lt/). Taigi, Lietuvos banko nuomone, pareiškėjai pateikta aktyvi nuoroda buvo pakankamai pastebima, kad yra klaidinga, ir pareiškėja turėjo susilaikyti nuo trečiųjų asmenų nurodymų vykdymo.

Vertinant tolimesnius pareiškėjos veiksmus pareiškėjai paspaudus aktyvią nuorodą ir patekus į trečiųjų asmenų suklastotą „Omniva" puslapį, pažymėtina, kad, kaip nurodė pareiškėja, ji per „Facebook" tikėjosi parduoti prekę ir už ją į savo sąskaitą gauti pinigines lėšas. Tai reiškia, kad pareiškėja neturėjo tikslo iš savo sąskaitos panaudojant savo mokėjimo priemonės duomenis įvykdyti Operacijas. Tačiau, siekdama už prekę gauti pinigus į savo banko sąskaitą, pareiškėja suvedė savo mokėjimo kortelės duomenis ir „Smart-ID" paskyros PIN1 kodą. Taigi, tam, kad pareiškėja tariamai į savo banko sąskaitą gautų pinigines lėšas, jos buvo prašoma suvesti personalizuotus duomenis, kurie įprastai suvedami norint inicijuoti ir patvirtinti mokėjimo operaciją iš banko sąskaitos.

Atkreiptinas dėmesys: kad piniginės lėšos būtų gautos į banko sąskaitą, bankai neprašo sąskaitos turėtojo pateikti savo mokėjimo kortelės duomenų ir neprašo suvesti „Smart-ID" programėlės PIN1 kodo. Taigi, pareiškėja, nors ir turėjo galimybę kritiškai įvertinti savo veiksmų su mokėjimo priemone riziką ir galimas pasekmes, tačiau nuo tolimesnių veiksmų nesusilaikė, o priešingai – vykdė trečiųjų asmenų nurodymus, netgi keletą kartų suvedė savo „Smart-ID" programėlės PIN1 kodą ir tokiais savo veiksmais patvirtino Operacijas.

Taigi, šiuo konkrečiu atveju vertinant pareiškėjos elgesį būtent nagrinėjamo ginčo aplinkybių ir prieš pareiškėją nukreiptos specifinės sukčiavimo atakos kontekste, esminėmis aplinkybėmis, vertinant pareiškėjos neatsargumo laipsnį, Lietuvos banko vertinimu, laikytina tai, kad pareiškėjai nesukėlė jokių įtarimų tai, kad jos yra prašoma pateikti visus būtent pačios pareiškėjos mokėjimo kortelės duomenis, kuriuos ji pripažįsta suvedusi, nors pati pareiškėja tik siekė gauti lėšas, o ne įvykdyti mokėjimo operaciją. Be to, pareiškėjai atsiųsta paslaugų teikėjo „Omniva" nuoroda buvo nepanaši į teisingą prisijungimo prie tikros bendrovės „Omniva" interneto svetainės nuorodą. Kaip minėta, pagal banko mokėjimo paslaugų teikimo sąlygas, mokėjimo kortelės personalizuotų saugumo duomenų pateikimas minėtose sąlygose numatytais atvejais laikomas kliento (šiuo atveju – pareiškėjos) sutikimu įvykdyti mokėjimo operaciją, lėšas nurašant iš kliento (šiuo atveju – pareiškėjos) sąskaitos. Atitinkamai ginčo

byloje nėra jokių duomenų ir kad pareiškėja būtų kvestionavusi pagal pranešime paspaustą nuorodą atsidariusio interneto puslapio autentiškumą, o jei tokių abejonių turėjo, nėra jokių duomenų, kad šias abejones būtų bandžiusi išsklaidyti, patikrinti gautą informaciją.

Be to, bankas viešai platino pranešimą ir įspėjo klientus apie tai, kad sukčiai siuntinėja įvairias žinutes, kurios gali neatitikti tikrovės ir kuriose yra pateikiamos netikros nuorodos, kurias paspaudę ir suvedę savo personalizuotus saugumo duomenis, klientai gali prarasti lėšas. Bankas ragino to neatlikti[7]. Taip pat bankas pateikė duomenis, kad pareiškėja 2023 m. vasario 15 d. ir 2023 m. gegužės 23 d. el. laiškais asmeniškai buvo įspėta, kad būtų budri, nes sukčiai aktyviai vilioja bankų klientų duomenis. Taigi, iš šių duomenų matyti, kad bankas prevenciškai dėjo pastangas tam, kad pareiškėja būtų supažindinta su sukčiavimo elektroninėje erdvėje rizikomis, taip pat tapatybės patvirtinimo priemonės saugaus naudojimo, jos personalizuotų saugumo žymenų suvedimo ir atskleidimo reikšme bei teisinėmis pasekmėmis.

Nesutikdama su banko pateiktais argumentais, pareiškėja nurodė, kad tam, kad Operacijos būtų patvirtintos, užteko suvesti „Smart-ID" paskyros PIN1 kodą, nors įprastai mokėjimo operacijoms patvirtinti reikia papildomai suvesti ir „Smart-ID" paskyros PIN2 kodą. Dėl šios priežasties, pareiškėjos nuomone, bankas netinkamai atliko visus veiksmus, todėl tretieji asmenys turėjo galimybę pasisavinti pareiškėjos lėšas. Vertinant tiek pareiškėjos, tiek banko pateiktus duomenis, svarbu pažymėti, kad, kaip ir minėta, Operacijos buvo atliktos pareiškėjos mokėjimo kortele. Sąlygų 7.2.8 papunktyje yra numatyta, kad „Kortelės turėtojas, atsiskaitydamas kortele už prekes / paslaugas elektroninėse prekybos vietose (internete), operaciją papildomai turi patvirtinti Kliento atpažinimo priemone. Kliento atpažinimo priemonių, tinkančių patvirtinti operacijas elektroninėse prekybos vietose (internete), sąrašas skelbiamas Banko interneto tinklalapyje ir / ar šiose Sąlygose." Iš Lietuvos bankui pateiktų duomenų matyti, kad pareiškėjai buvo taikytas saugesnio autentiškumo patvirtinimas[8], t. y. buvo taikomi žinojimo ir turėjimo elementai. Tiek iš pareiškėjos pateiktų paaiškinimų, tiek iš banko pateiktų objektyvių duomenų matyti, kad pareiškėja turėjo pateikti vardą, pavardę, mokėjimo kortelės numerį ir CVV kodą (žinojimo elementas), o vėliau suvesti „Smart-ID" paskyros PIN1 kodą (turėjimo elementas). Taigi, atsižvelgiant į šiuos duomenis, darytina išvada, kad bankas pagrįstai, vadovaudamasis Sąlygų nuostatomis, Operacijoms patvirtinti reikalavo suvesti tik „Smart-ID" paskyros PIN1 kodą, o pareiškėjos pateikti argumentai yra atmesti kaip nepagrįsti.

Išanalizavęs šias bei visas kitas ginčo nagrinėjimo metu nustatytas aplinkybes ir ginčo byloje esančius duomenis, Lietuvos bankas daro išvadą, kad vis dėlto vertinti pareiškėjos elgesio kaip atsargaus ir apdairaus ar tik neatsargaus šiuo atveju nėra galima.

Kaip matyti iš ginčo nagrinėjimo metu nustatytų aplinkybių, Operaciją tretieji asmenys be pareiškėjos žinios galėjo atlikti tik dėl to, kad pareiškėja, būdama labai neatsargi, netinkamai įvykdė Mokėjimų įstatyme (34 straipsnis) ir su banku sudarytoje mokėjimo kortelės sutartyje įtvirtintus mokėjimo kortelės saugaus naudojimo reikalavimus. Remiantis nustatytais duomenimis, tam, kad pareiškėja parduotų prekę, jai nebuvo būtina suvesti savo mokėjimo kortelės duomenų ir „Smart-ID" paskyros PIN1 kodo. Tačiau pareiškėja, gavusi trečiųjų asmenų siųstą pranešimą, nedvejodama (kaip pripažįsta) paspaudė jame pateiktą nuorodą ir suklastotame interneto puslapyje nurodė savo mokėjimo kortelės personalizuotus saugumo duomenis, neįsitikinusi nei siųsto pranešimo ir jame pateiktos nuorodos, nei į ją nukreipiančios interneto svetainės autentiškumu bei prašymo atskleisti konfidencialius savo mokėjimo priemonių duomenis tikrumu. Taip pat pareiškėja, nepatikrinusi kontrolinio kodo ir neatsižvelgusi į tai, kad siekia gauti lėšas, o ne jas pervesti, galiausiai patvirtino Operacijas.

Nurodytos aplinkybės leidžia teigti, kad pareiškėja būtent dėl savo didelio neatsargumo neišsaugojo jos vardu išduotos mokėjimo kortelės duomenų konfidencialumo – nesiėmė tų saugumo priemonių, kurių privalėjo imtis, kad būtų tinkamai apsaugoti jai suteiktos mokėjimo priemonės duomenys, ir pati patvirtino Operacijas.

Konstatavus, kad pareiškėja, nesilaikydama jai, kaip mokėtojai, Mokėjimų įstatyme ir sutartyje su banku nustatytų pareigų, susijusių su 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

[7] https://www.luminor.lt/lt/naujienos/luminor-ispeja-klientus-sukciai-siuntineja-melagingas-trumpasias-zinutes

[8] Sąlygų 3.1 papunkčio 46 dalyje nustatyta, kad Saugesnis autentiškumo patvirtinimas – autentiškumo patvirtinimas, kai saugiai naudojami bent du į žinojimo (tai, ką žino tik Klientas), turėjimo (tai, ką turi tik Klientas) ir būdingumo (tai, kas būdinga tik Klientui) kategorijas skirstomi elementai, o pažeidus vieną elementą neturi sumažėti kitų elementų patikimumas.

pareigos grąžinti (kompensuoti) pareiškėjai neautorizuotų Operacijų lėšų.

Įvertinus visa tai, kas išdėstyta pirmiau, ir nustačius, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, darytina išvada, kad pareiškėjos bankui keliamas reikalavimas grąžinti ir (ar) kompensuoti Operacijų sumą – 3 751,13 Eur, yra nepagrįstas, todėl atmetamas.

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 pareiškėjos X. X. reikalavimą.

Lietuvos banko sprendimas dėl ginčo esmės yra rekomendacinio pobūdžio ir teismui neskundžiamas. Vartotojui ir finansų rinkos dalyviui išlieka teisė dėl tapataus ginčo dalyko kreiptis į teismą įstatymų nustatyta tvarka. Kreipimasis į teismą po Lietuvos banko sprendimo dėl ginčo esmės priėmimo nelaikomas šio sprendimo apskundimu. Ginčo šalys turi pareigą pranešti Lietuvos bankui, jeigu viena iš ginčo šalių pareiškia ieškinį bendrosios kompetencijos teismui prašydama nagrinėti tapatų ginčą iš esmės.

Direktorius Arūnas Raišutis