



**LIETUVOS BANKO
TEISĖS IR LICENCIJAVIMO DEPARTAMENTO
DIREKTORIUS**

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

2022-08-26 Nr. 429-411
Vilnius

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

N u s t a t y t a:

2022 m. gegužės 7–8 d. iš pareiškėjos sąskaitos banke pareiškėjai banko išduota mokėjimo kortele buvo inicijuota dvylika mokėjimo operacijų įvairiems gavėjams. Bendra mokėjimo operacijų suma – 3 714,85 Eur (toliau – mokėjimo operacijos). Septynios mokėjimo operacijos buvo inicijuotos pareiškėjos mokėjimo kortelę pridėjus prie elektroninės pinigines panaudojant *Apple Pay* atsiskaitymo metoda, o kitos šešios – suvedus mokėjimo kortelės duomenis ir mokėjimo operacijų įvykdymą patvirtinus pareiškėjos mobiliuoju parašu.

2022 m. gegužės 8 d. pareiškėja telefonu kreipėsi į banką ir informavo, kad ji galėjo tapti trečiųjų asmenų neteisėtų veiksmų auka, todėl prašė banko blokuoti mokėjimo kortelę, stabdyti ir atšaukti mokėjimo operacijas, o jos banko sąskaitoje rezervuotas mokėjimo operacijų lėšas gražinti pareiškėjai. Pareiškėja bankui teigė, kad mokėjimo operacijas patvirtino ji pati.

2022 m. gegužės 10 d. bankas pareiškėją informavo, kad negali atšaukti pareiškėjos banko sąskaitoje rezervuotų mokėjimo operacijų lėšų. Bankas pareiškėjai paaiškino, kad pareiškėjos mokėjimo operacijos buvo pavirtintos banko ir pareiškėjos sutartu būdu, todėl bankas pagrįstai įvykdė mokėjimo operacijas.

Pareiškėja, nesutikdama su banko atsakymu, kreipėsi į Lietuvos banką dėl vartojimo ginčo nagrinėjimo. Kreipimesi pareiškėja paaiškino, kad „2022 m. gegužės mėn. 8 d. naudodamasi *Vinted* programėle (parduodant prekę) gavau pranešimą kuriame buvo prašoma mano el. pašto adreso, kad būtų galima užbaigti pirkimą ir pervesti pinigus į mano sąskaitą. Davus el. pašto adresą gavau į jį nuorodą, kurią reikėjo paspausti ir suvedus mano banko kortelės duomenis tariamai gauti pinigus už parduodamą prekę. Šios operacijos metu telefono ekrane buvo virtualaus asistento langas kurio buvo neįmanoma uždaryti, o už jo buvo matyti, kad kažkas vyko, tačiau nesimatė kas. Suvedus kortelės duomenis pasirodė keturių skaitmenų kodas, kurį turėjau patvirtinti elektroniniu parašu. Tai kartojosi kelis kartus. Po kurio laiko pastebėjau, kad mano sąskaitos likutis gerokai sumažėjo ir tada nedelsiant paskambinau į banką kad blokuotų mokėjimo kortelę. Toks pat procesas vyko ir gegužės 7 d., tačiau tuo momentu įtarimo kažkaip nekilo, nes buvo svečių, šurmulyš ir mintys nebuvo koncentruotos į tai, kas vyksta.“ Pareiškėja prašė rekomenduoti bankui gražinti 3 714,85 Eur mokėjimo operacijų sumą.

Bankas Lietuvos bankui pateiktame atsiliepime paaiškino, kad dalis mokėjimo operacijų buvo inicijuotos pareiškėjos mokėjimo kortelę pridėjus prie *Apple Pay* ir konkrečią mokėjimo operaciją patvirtinus panaudojant *Apple Pay* mokėjimo metoda, o kita dalis mokėjimo operacijų buvo inicijuotos suvedus mokėjimo kortelės duomenis ir konkrečią mokėjimo operaciją patvirtinus mobiliuoju parašu. Banko teigimu, pačios pareiškėjos elgesys, dėl kurio ji prarado savo mokėjimo priemonę, o tretieji asmenys įgijo galimybę iš pareiškėjos sąskaitos be pareiškėjos žinios ir sutikimo inicijuoti mokėjimo operacijas, buvo labai neatsargus. Kaip teigia bankas, pareiškėja nesilaikė minimalių atsargumo reikalavimų, o tai ir lėmė, kad ji atskleidė savo personalizuotus saugos duomenis tretiesiems asmenims: pareiškėja, gavusi trečiųjų asmenų atsiųstą aktyvią nuorodą, ją paspaudė ir joje suvedė savo mokėjimo kortelės duomenis (CVV / CVC kodą, kortelės numerį ir galiojimo datą), iš banko savo telefono numeriu SMS žinute

gavusi vienkartinį saugos kodą, skirtą mokėjimo kortelei pridėti prie *Apple Pay*, jį suvedė, dėl to tretieji asmenys įgijo galimybę pareiškėjos mokėjimo kortelę pridėti prie elektroninės piniginių ir inicijuoti mokėjimo operacijas panaudodami *Apple Pay* mokėjimo metodą. Taip pat dalį mokėjimo operacijų pareiškėja patvirtino suvedama savo mokėjimo kortelės duomenis ir mokėjimo operacijų įvykdymą patvirtindama mobiliuoju parašu. Banko teigimu, pareiškėjos didelį aplaidumą prarandant mokėjimo priemonę įrodo tai, kad pareiškėjai nekilo jokių įtarimų dėl to, kad jos atidarytoje nuorofoje neva į *Vinted* platformos interneto svetainę pateikiama informacija buvo su klaidomis, o pati pareiškėjos naršyklė, prieš pareiškėjai atidarant nuorodą, siuntė įspėjimą apie tai, kad interneto svetainė, į kurią ji pateko, yra nesaugi.

Bankas, atsakydamas į pareiškėjos reikalavimą atšaukti mokėjimo operacijas, paaiškino, kad galimybių atšaukti banko ir pareiškėjos sutartu būdu patvirtintas mokėjimo operacijas po to, kai bankas gavo mokėjimo nurodymus, neturėjo. Bankas pažymėjo, jog tam, kad mokėjimo operacijas galėtų atšaukti, yra būtinas lėšų gavėjo sutikimas, t. y. bankas savo iniciatyva negali atšaukti mokėjimo operacijų ir panaikinti lėšų rezervacijos pareiškėjos banko sąskaitoje.

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 pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Pareiškėjos ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjai jos vardu banke atidarytoje sąskaitoje kortele atliktų mokėjimo operacijų lėšas, iš viso 3 714,85 Eur. Pareiškėja teigia neautorizavusi (nenorėjusi įvykdyti) mokėjimo operacijų, tačiau ir neneigia trečiųjų asmenų suklastotoje *Vinted* interneto svetainėje pati suvedusi savo mokėjimo kortelės duomenis, banko SMS žinute gautą vienkartinį saugos kodą, kuriuo buvo patvirtintas mokėjimo kortelės pridėjimas prie elektroninės piniginių, bei savo mobiliajame telefone suvedusi savo mobiliojo parašo duomenis, kuriais patvirtino konkrečių mokėjimo operacijų įvykdymą. Pareiškėjos teigimu, tuo metu, kai ji kreipėsi į banką ir prašė blokuoti jos mokėjimo kortelę, mokėjimo operacijų lėšos pareiškėjos sąskaitoje buvo dar tik rezervuotos, todėl bankas galėjo atšaukti mokėjimo operacijų įvykdymą ir grąžinti pareiškėjai mokėjimo operacijų lėšas. Bankas teigia, kad pareiškėjos mokėjimo operacijos buvo patvirtintos šalių sutarta forma ir tvarka, dėl to bankas jas pagrįstai įvykdė, o pareiškėja į banką dėl mokėjimo operacijų atšaukimo kreipėsi po to, kai mokėjimo nurodymai buvo gauti banke, todėl bankas mokėjimo operacijų be gavėjo sutikimo atšaukti negalėjo. Taip pat bankas teigia, kad yra sąlygos pareiškėjos elgesį, prarandant savo mokėjimo priemonę, vertinti kaip labai neatsargų, todėl bankas mano, kad neturi pareigos kompensuoti pareiškėjai jos patirtų nuostolių dėl mokėjimo operacijų įvykdymo. Dėl šių priežasčių, banko nuomone, visi mokėjimo operacijų nuostoliai turėtų tekti pareiškėjai.

Tarp šalių nėra ginčo dėl to, kad mokėjimo operacijoms įvykdyti nebuvo duotas pareiškėjos sutikimas, t. y. tiek pareiškėja, tiek bankas pripažįsta, kad mokėjimo operacijas inicijavo ne pati pareiškėja, o tretieji asmenys, neteisėtu būdu pasisavinę pareiškėjos mokėjimo priemonę. Taip pat svarbu tai, kad pareiškėja, nors ir teigia, kad ji neturėjusi tikslo iš savo banko sąskaitos įvykdyti konkrečių mokėjimo operacijų gavėjams ir jų pati neinicijavo, visgi pripažįsta, jog suvedama savo personalizuotus saugos duomenis patvirtino mokėjimo operacijų įvykdymą.

Taip pat svarbu tai, kad ginčo byloje ginčo šalių pateikti paaiškinimai apie mokėjimo operacijų įvykdymą leidžia teigti, jog mokėjimo operacijas galėjo inicijuoti ne pati pareiškėja, bet tretieji asmenys, neteisėtu būdu pasisavinę pareiškėjos mokėjimo priemonę. Atsižvelgiant į tai, kad iš esmės abi ginčo šalys sutaria, kad mokėjimo operacijos galėjo būti inicijuotos be pačios pareiškėjos valios, o trečiųjų asmenų iniciatyva, toliau sprendime nebus analizuojamos su mokėjimo operacijų autorizavimo vertinimu susijusios aplinkybės, o mokėjimo operacijos laikomos pareiškėjos neautorizuotomis.

Ginčo šalys iš esmės nesutaria dėl to, kam turėtų tekti atsakomybė už neautorizuotų mokėjimo operacijų įvykdymą: bankas teigia, kad pareiškėjos elgesys, tretiesiems asmenims atskleidžiant savo personalizuotus saugos duomenis ir prarandant savo mokėjimo priemonę,

buvo labai neatsargus. Pareiškėja neneigia pati trečiųjų asmenų suklastotoje *Vinted* platformos svetainėje suvedusi savo mokėjimo kortelės duomenis, iš banko SMS žinute gautą vienkartinį saugos kodą, kuris buvo skirtas mokėjimo kortelei pridėti prie elektroninės piniginės, bei savo mobiliajame telefone suvedusi mobiliojo parašo duomenis, kuriais buvo patvirtintas konkrečių mokėjimo operacijų įvykdymas, tačiau teigia, kad bankas, jai kreipusis dėl mokėjimo operacijų atšaukimo, turėjo jas atšaukti ir sugrąžinti jai mokėjimo operacijų lėšas.

Siekiant išspręsti tarp pareiškėjos ir banko kilusį ginčą, Lietuvos banko vertinimu, būtina nustatyti šias pagrindines aplinkybes: 1) ar bankas turėjo (turi) pareigą grąžinti pareiškėjai neautorizuotų mokėjimo operacijų sumas; 2) ar bankas turėjo pareigą atšaukti mokėjimo operacijas.

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 neautorizuotų mokėjimo operacijų pasekmių ir pareiškėjos teisės į mokėjimo operacijų sumos grąžinimą

Vadovaudamasis Mokėjimų įstatymo 38 straipsnio 1 dalimi, mokėtojo mokėjimo paslaugų teikėjas privalo grąžinti 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 pagrįstų priežasčių įtarti mokėtojo sukčiavimą ir apie šias priežastis raštu praneša priežiūros institucijai (Lietuvos bankui).

Pagal Mokėjimų įstatymo 39 straipsnio 1 dalį, mokėtojui gali tekti dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai iki 50 eurų, 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 jis iki mokėjimo operacijos įvykdymo negalėjo pastebėti mokėjimo priemonės praradimo, vagystės arba neteisėto pasisavinimo, išskyrus atvejus, kai jis veikė nesąžiningai (1 punktas). 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. Tokiais atvejais Mokėjimų įstatymo 39 straipsnio 1 dalyje nustatytas didžiausias nuostolių sumos ribojimas netaikomas.

Pagal Mokėjimų įstatymo 2 straipsnio 32 dalį, mokėjimo priemonė – personalizuota priemonė ir (arba) tam tikros procedūros, dėl kurių susitaria mokėjimo paslaugų vartotojas ir mokėjimo paslaugų teikėjas ir kurias mokėjimo paslaugų vartotojas naudoja mokėjimo nurodymui inicijuoti. Pasisavinimas šiuo atveju turėtų būti suprantamas kaip svetimos mokėjimo priemonės užvaldymas ir galėjimas ja naudotis kaip sava. Neteisėtumas suponuoja atlikto veiksmo teisinio pagrindo nebuvimą.

Bankas teigia, kad tretieji asmenys neteisėtu būdu galėjo pasisavinti pareiškėjos mokėjimo kortelės duomenis bei kitus personalizuotus saugos duomenis tik todėl, kad pareiškėja dėl savo didelio neatsargumo neįvykdė Mokėjimų įstatymo 34 straipsnyje numatytų mokėtojo pareigų ir neužtikrino, kad, be pareiškėjos, turinčios teisę naudotis mokėjimo priemone, personalizuotais saugumo duomenimis negalėtų pasinaudoti kiti asmenys.

Kaip minėta, tiek pareiškėjos, tiek banko paaiškinimai apie mokėjimo operacijų įvykdymo aplinkybes iš esmės sutampa, o banko pateikti sistemų išrašai patvirtina ginčo šalių pateiktus paaiškinimus apie mokėjimo operacijų įvykdymo aplinkybes.

Ginčo byloje nustatyta, kad pareiškėja prarado savo mokėjimo priemonę, kai gavusi iš trečiųjų asmenų jai elektroniniu paštu skirtingomis dienomis (2022 m. gegužės 7 d. ir 2022 m. gegužės 8 d.) atsiųstas skirtingo turinio žinutes su skirtingomis nuorodomis, jas atidarė ir, patekusi į vizualiai panašią į tikrąją *Vinted* platformos svetainę, joje suvedė savo mokėjimo kortelės duomenis. Ginčo byloje nustatytais duomenimis, pareiškėja 2022 m. gegužės 7 d. savo elektroninio pašto adresu gavo pranešimą, kuriame buvo nurodoma tokia informacija: „Sveiki. Jūsų prekė buvo įsigyta saugiu sandoriu vinted.lt. Norėdami užbaigti sandorį ir gauti pinigus, turite spustelėti nuorodą. Iškart po to su jumis susisieks vinted.lt kurjerių tarnyba ir aptars siuntos pristatymo datą. Siuntinį galite išsiųsti bet kuriuo jums patogiu metu.“ Pareiškėja teigė, kad ji paspaudė minėtoje žinutėje pateiktą aktyvią nuorodą (vinted.lt) ir joje suvedė savo

mokėjimo kortelės duomenis. Banko pateiktais duomenimis, 2022 m. gegužės 7 d. 16:52 val. pareiškėja savo mobiliojo telefono numeriu iš banko gavo SMS žinutę su tokiu pranešimo tekstu: „Iveskite koda *duomenys neskelbiami* noredami pridėti kortele i skaitmenine pinigine. Sis kodas galios 30 minuciu. Luminor“. Pareiškėja neneigia suvedusi šį kodą. Banko pateiktais duomenimis, 16:52 val. pareiškėja savo mobiliuoju telefonu gavo SMS žinutę su tokiu pranešimo tekstu: „Jusu Luminor kortele, kurios numeris baigiasi *duomenys neskelbiami* yra paruosta Google Pay naudojimui. Ji galite naudoti visur, kur matote bekontaktį simboli arba Google Pay zenkla. Luminor“. Pareiškėja teigė, kad į šias žinutes tuo metu neatkreipė dėmesio. 2022 m. gegužės 7 d. pareiškėjos suvestus mokėjimo kortelės duomenis nusavino tretieji asmenys ir inicijavo pareiškėjos mokėjimo kortelės pridėjimą prie *Apple Pay*, kurį pareiškėja patvirtino suvesdama banko jai SMS žinute atsiųstą vienkartinį saugos kodą.

2022 m. gegužės 8 d. pareiškėja savo elektroniniu paštu gavo dar vieną žinutę, kurioje jai buvo pranešta, kad jos parduodama prekė buvo sėkmingai įsigyta ir tam, kad pareiškėja už prekę gautų pinigus, ji turi paspausti pateiktą aktyvią nuorodą „priimti lėšas“. Pareiškėja, paspaudusi jai pateiktą aktyvią nuorodą, joje suvedė savo mokėjimo kortelės duomenis ir konkrečias mokėjimo operacijas (iš viso 6) patvirtino savo mobiliajame telefone suvesdama mobiliojo parašo duomenis.

Pagal ginčo byloje pareiškėjos pateiktus paaiškinimus, spausdama trečiųjų asmenų jai atsiųstose žinutėse pateiktas aktyvias nuorodas ir patekusi neva į *Vinted* platformos svetainę ir joje vesdama savo kortelės duomenis ji tikėjosi už prekę gauti pinigus į savo sąskaitą banke. Kaip pati pareiškėja teigia, vesdama savo mokėjimo kortelės duomenis ji savo telefono ekrane pastebėjo neįprastus veiksmus (virtualaus asistento langą, kurio negalėjo uždaryti), tačiau vis tiek toliau tęsė jos trečiųjų asmenų prašomus atlikti veiksmus ir kelis kartus suvedė savo mobiliojo parašo duomenis bei SMS žinute banko jai atsiųstą vienkartinį saugos kodą. Pareiškėja paaiškino, kad 2022 m. gegužės 7 d. atlikdama veiksmus su savo mokėjimo priemone ji nesikoncentravo į juos, „toks pat procesas vyko ir gegužės 7 d., tačiau tuo momentu įtarimo kažkaip nekilo, nes buvo svečių, šurmulyš ir mintys nebuvo koncentruotos į tai, kas vyksta“.

Teigdamas, kad pareiškėjos elgesys, dėl kurio ji prarado savo mokėjimo priemonę, turi didelio neatsargumo požymių, bankas remiasi tuo, kad pareiškėja nesilaikė mokėtojai nustatytos pareigos saugoti personalizuotus saugos duomenis ir niekam jų neatskleisti. Banko teigimu, pareiškėjai turėjo kilti įtarimų dėl gaunamų nuorodų tikrumo, nes pranešimų tekstai buvo parašyti su gramatinėmis klaidomis, siuntėjo *Vinted* elektroninio pašto adresas „@gmail.com“. Taip pat ir pačios pareiškėjos naršyklė pareiškėją įspėjo apie tai, kad interneto svetainė, į kurią pareiškėja pateko, gali būti nesaugi.

Lietuvos bankas pažymi, kad didelis neatsargumas ar paprastas neatsargumas yra vertinamojo pobūdžio aplinkybės, todėl išvada dėl mokėtojo elgesio vertinimo kaip neatsargaus ar labai neatsargaus dėl neautorizuotos mokėjimo operacijos ar dėl mokėjimo priemonės praradimo, lėmusio neautorizuotą mokėjimo operaciją, darytina kiekvienu konkrečiu atveju, įvertinus nustatytų individualių, specifinių aplinkybių visumą, kurią patvirtina ginčo byloje esantys įrodymai ir (arba) yra šalių neginčijamos neautorizuotos mokėjimo operacijos įvykdymo aplinkybės. Taigi, išvada dėl mokėtojo paprasto ar didelio neatsargumo, kaip vertinamojo pobūdžio aplinkybė, negali būti daroma izoliuotai, išsamiai neįvertinus viso neautorizuotos mokėjimo operacijos įvykdymo ir su juo susijusių aplinkybių konteksto.

Kriterijai, į kuriuos reikėtų atsižvelgti vertinant kaltės laipsnį, yra iš dalies suformuluoti Antrosios mokėjimo paslaugų direktyvos preambulės 72 punkte: „Siekiant įvertinti galimą mokėjimo paslaugų vartotojo aplaidumą ar didelį aplaidumą, reikėtų atsižvelgti į visas aplinkybes. Įtariamo aplaidumo įrodymai ir laipsnis paprastai turėtų būti vertinami pagal nacionalinę teisę. Tačiau nors aplaidumo sąvoka reiškia, kad pažeidžiamas įsipareigojimas elgtis rūpestingai, didelis aplaidumas turėtų reikšti daugiau nei vien aplaidumą ir apimti labai nerūpestingą elgesį; pavyzdžiui, tai būtų mokėjimo operacijos autorizavimui naudojamų saugumo požymių laikymas prie mokėjimo priemonės atviru ir trečiosioms šalims lengvai atskleidžiamu formatu.“

Didelio neatsargumo sąvoka taip pat plėtojama Lietuvos Aukščiausiojo Teismo praktikoje. Kasacinis teismas yra išaiškinęs, kad „didelis neatsargumas kaip kaltės forma pasireiškia neprotingu arba išskirtiniu rūpestingumo nebuvimu, kai asmuo nėra tiek rūpestingas, kiek akivaizdžiai būtina esamomis aplinkybėmis“ (Lietuvos Aukščiausiojo Teismo 2017 m. balandžio 13 d. nutartis civilinėje byloje Nr. e3K-3-180-378/2017, 29 punktas).

Vertinant, ar pareiškėjos elgesys, kai ji paspaudė jos elektroniniu paštu atsiųstose

žinutėse esančias aktyvius nuorodas ir tikslu gauti pinigines lėšas į savo banko sąskaitą suvedė savo mokėjimo kortelės duomenis, savo mobiliojo telefono numeriu SMS žinute gautą vienkartinį saugos kodą, o vėliau ir savo mobiliojo parašo duomenis, gali būti vertinamas kaip labai neatsargus pareiškėjos elgesys, t. y. toks elgesys, dėl kurio mokėjimo priemonės turėtojo veiksmai iš esmės skiriasi nuo atsargaus elgesio reikalavimų, pažymėtina, kad vien tik faktas, jog pareiškėja paspaudė jai žinute atsiųstą aktyvią nuorodą ir nepastebėjo, kad pateko ne į tikrą *Vinted* platformos interneto svetainę, o į trečiųjų asmenų suklastotą *Vinted* platformos interneto svetainę, savaime nereiškia pareiškėjos didelio neatsargumo. Nagrinėjamo ginčo atveju pareiškėja iš trečiųjų asmenų gavo dvi skirtingo turinio žinutes su pateiktomis skirtingomis aktyviomis nuorodomis. Vertinant pareiškėjai 2022 m. gegužės 7 d. pateiktos žinutės turinį galima matyti, kad žinutė yra parengta lietuvių kalbos rašmenimis, be aiškiai matomų gramatinių klaidų. Todėl pareiškėjai objektyviai galėjo atrodyti, kad minėtą žinutę jai siuntė tikroji *Vinted* platforma. Tačiau vertinant 2022 m. gegužės 8 d. pareiškėjai siųstos žinutės turinį matyti, kad vizualiai ji atrodė kitokia nei 2022 m. gegužės 7 d. siųstoji, joje informacija buvo pateikiama ne tik lietuvių, bet ir lenkų kalbomis. Tačiau pačios žinutės vizualus dizainas buvo labai panašus į tikrosios *Vinted* platformos dizainą. Vertinant aplinkybių visumą, nors ir būtų galima teigti, kad pareiškėja galėjo pastebėti, jog iš tos pačios neva *Vinted* platformos jai siųstų žinučių turinys ir vaizdas skyrėsi, tačiau atsižvelgiant į tai, kad žinutės buvo parašytos lietuviškais rašmenimis be didelių gramatinių klaidų, o vizualus žinutės dizainas buvo panašus į tikrąją *Vinted* platformą, pareiškėjai pagrįstai galėjo atrodyti, kad minėtas žinutes siuntė tikroji *Vinted* platforma ir tai galėjo sumažinti pareiškėjos budrumą.

Vertinant tolesnius pareiškėjos veiksmus jai paspaudus aktyvius nuorodas ir patekus į trečiųjų asmenų suklastotą *Vinted* platformos svetainę, visų pirma pažymėtina, kad pareiškėja jai elektroniniu paštu siųstuose pranešimuose gavo informaciją, jog jos per *Vinted* platformą parduodamos prekės buvo nupirktos ir tam, kad pareiškėja už prekes gautų pinigus į savo banko sąskaitą, ji turi suvesti savo mokėjimo kortelės duomenis ir patvirtinti lėšų į banko sąskaitą įskaitymą. Taigi tam, kad pareiškėja į savo banko sąskaitą gautų pinigines lėšas, jos buvo prašoma suvesti personalizuotus duomenis, kurie įprastai yra reikalingi norint inicijuoti ir patvirtinti mokėjimo operaciją iš banko sąskaitos. Pažymėtina, kad norint gauti pinigines lėšas į savo banko sąskaitą bankai neprašo tuo tikslu pateikti savo mokėjimo kortelės duomenų, neprašo suvesti mobiliojo parašo duomenų, SMS žinute nesiunčia vienkartinio saugos kodo ir neprašo jo suvesti siekiant mokėjimo kortelę pridėti prie skaitmeninės piniginės. Tačiau pareiškėjai faktas, kad tikslu į savo sąskaitą gauti pinigines lėšas jos buvo prašoma suvesti duomenis, kurie iš esmės yra reikalingi atlikti priešingą veiksma – patvirtinti lėšų iš banko sąskaitos nurašymą, nesukėlė jokių įtarimų ir pareiškėja keletą kartų dviejų dienų laikotarpiu vykdė trečiųjų asmenų nurodymus jų nevertindama kritiškai. Pareiškėja paaiškino, kad atlikdama minėtus veiksmus nebuvo labai atidi, savo mobiliojo telefono ekrane matė virtualaus asistento langą, kurio niekaip negalėjo uždaryti, ir iš esmės visus veiksmus atliko gerai nematydama, kokius veiksmus ji tvirtino. Pareiškėja 2022 m. gegužės 7 d. iš banko gavo SMS žinutę su vienkartinio saugos kodu, kuriame buvo aiškiai pateikta informacija apie tai, kad šis saugos kodas yra skirtas kortelei pridėti prie skaitmeninės piniginės. Tačiau pareiškėja nekreipė dėmesio į šios banko žinutės turinį, kurioje iš esmės buvo aiškiai parašytas vienkartinio saugos kodo siuntimo tikslas – pridėti mokėjimo kortelę prie skaitmeninės piniginės, o ne įskaityti mokėjimo operacijos lėšas, kaip manė pareiškėja. Pareiškėja ir 2022 m. gegužės 8 d. mokėjimo operacijų įvykdymą net kelis kartus patvirtindama savo mobilioju parašu kritiškai nevertino savo atliekamų veiksmų, nors ir teigė, kad telefono ekrane jai buvo matyti virtualus asistentas, kurio lango ji niekaip negalėjo uždaryti, dėl to ji iki galo nematė, kas iš tikrųjų vyksta su jos banko sąskaita. Nors pareiškėjai ir pasirodė neįprasta, kad jos telefono ekrane atsirado virtualaus asistento langas, kurį pareiškėja mėgino uždaryti tam, kad pamatytų, kokius veiksmus ji iš tikrųjų tvirtina suveddama savo personalizuotus saugos duomenis, tačiau pareiškėja nesustabdė savo veiksmų ir toliau atliko visus trečiųjų asmenų jos prašomus atlikti veiksmus – suvedė mokėjimo kortelės duomenis, mokėjimo kortelės pridėjimą prie virtualios piniginės patvirtino suveddama vienkartinį saugos kodą bei net keletą kartų iš eilės savo mobilijame telefone suvedė elektroninio parašo duomenis ir taip patvirtino mokėjimo operacijų įvykdymą. Pažymėtina, kad pareiškėja šiuos veiksmus atliko dviejų dienų laikotarpiu, t. y. pareiškėja turėjo pakankamai laiko jau po 2022 m. gegužės 7 d. pasitikrinti savo banko sąskaitą ir, jeigu pareiškėja būtų buvusi atidi ir rūpestinga ir jau 2022 m. gegužės 7 d. pasitikrinusi savo banko sąskaitą, ji būtų pastebėjusi iš jos banko sąskaitos be jos žinios ir sutikimo įvykdytas mokėjimo operacijas. Tikėtina, kad pareiškėja būtų išvengusi ir 2022 m. gegužės 8 d. be jos

žinios ir sutikimo mokėjimo operacijų iš jos banko sąskaitos įvykdymo.

Banko Mokėjimo paslaugų teikimo sąlygų (toliau – Sąlygos) 6.3.1 papunktyje 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 prigludimas prie specialiu ženklu 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. Sutikimą atlikti mokėjimo operaciją, o taip pat ir suteikti duomenis, reikalingus atlikti mokėjimo operacijai, taip pat galima pateikti (i) prigludžiant Kortelę ar įrenginį, turintį Skaitmeninę piniginę, kuri susieta su Kortele, prie mokėjimo terminalo bei autorizuojant mokėjimą įrenginyje nustatytu autorizacijos metodu; (ii) atliekant veiksmus, nurodytus Skaitmeninės piniginės paslaugų teikėjo, norint patvirtinti mokėjimo operaciją naudojantis Skaitmenine pinigine. 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.“

Kaip matyti, banko mokėjimo paslaugų teikimo sąlygos aiškiai reglamentuoja, kad banko klientui suteikti personalizuoti duomenys yra naudojami duoti sutikimą įvykdyti mokėjimo operaciją. Ginčo byloje nėra duomenų apie tai, kad pareiškėja būtų buvusi nesupažindinta su Sąlygomis ar kad būtų jų nesupratusi. Taigi, pareiškėja iš esmės galėjo suprasti, kad tiek mokėjimo kortelės duomenų suvedimas, tiek ir mobiliojo parašo naudojimas gali lemti tam tikras teises pasekmes, šiuo atveju – mokėjimo priemonės praradimą ir neautorizuotų mokėjimo operacijų iš jos banko sąskaitos įvykdymą.

Lietuvos banko nuomone, jeigu pareiškėja būtų buvusi pakankamai atidi ir kritiška tiek žinutėmis gautos informacijos atžvilgiu, tiek savo atliekamų veiksmų atžvilgiu, būtų pastebėjusi, kad jos prašoma atlikti veiksmus, kurių nėra įprastai prašoma atlikti norint pinigines lėšas gauti į savo sąskaitą, o priešingai, yra prašoma atlikti veiksmus, kurie įprastai atliekami norint įvykdyti mokėjimo operacijas iš banko sąskaitos. Banko pareiškėjai siųstoje SMS žinutėje su vienkartinio saugos kodu buvo aiškiai nurodyta, kad vienkartinis saugos kodas yra skirtas mokėjimo kortelei pridėti prie skaitmeninės piniginės. Net jeigu pareiškėja neturėjo pakankamai žinių ir nesuprato, kaip veikia skaitmeninės piniginės paslauga, ji turėjo kritiškai įvertinti banko SMS žinutėje pateiktą informaciją apie vienkartinio saugos kodo paskirtį ir susilaikyti nuo tolesnių veiksmų. Pareiškėja taip pat turėjo kritiškai įvertinti faktą, kad jos buvo prašoma suvesti mobiliojo parašo duomenis, nors ji pati ir nesiekė inicijuoti jokių mokėjimo operacijų ar patvirtinti kažkokių kitų veiksmų, kuriems reikalingas pareiškėjos parašas, o tik siekė gauti lėšas į savo sąskaitą, kai lėšoms įskaityti į sąskaitą nereikia suvesti savo personalizuotų saugos duomenų. Taigi, jeigu pareiškėja būtų buvusi pakankamai atidi ir rūpestinga savo su mokėjimo priemone atliekamų veiksmų atžvilgiu, ji būtų galėjusi pastebėti trečiųjų asmenų neteisėtus veiksmus ir, labai tikėtina, būtų išvengusi neautorizuotų mokėjimo operacijų iš jos banko sąskaitos įvykdymo. Tačiau pareiškėja elgėsi nerūpestingai ir toliau vykdė trečiųjų asmenų jai pateiktus nurodymus. Pareiškėja elgėsi nerūpestingai ir net, kaip pati teigė, pastebėjusi neįprastus veiksmus (pvz., atsiradusį virtualaus asistento langą ir faktą, kad negalėjo jo uždaryti), nesulaukė nuo tolesnių veiksmų, nesikreipė į banką ir nepranešė bankui apie galimus neteisėtus trečiųjų asmenų veiksmus jos paskyroje, o priešingai, vykdė visus jai trečiųjų asmenų pateiktus nurodymus – ne tik suvedė personalizuotus saugos duomenis, reikalingus mokėjimo kortelei pridėti prie elektroninės piniginės, bet ir savo elektroniniu parašu patvirtino kelias iš eilės mokėjimo operacijas. Lietuvos banko vertinimu, toks pareiškėjos elgesys gali būti pripažintas kaip elgesys, iš esmės besiskiriantis nuo atsargaus elgesio reikalavimų, kuris galiausiai ir lėmė, kad pareiškėja prarado savo mokėjimo priemonę, o tretieji asmenys įgijo galimybę pareiškėjos vardu inicijuoti mokėjimo operacijas.

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) sužinotus 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 (2 dalis). Taigi, įvertinus ginčo byloje turimus duomenis bei ginčo šalių paaiškinimus apie mokėjimo operacijų įvykdymo aplinkybes, galima teigti, kad pareiškėja mokėjimo priemone naudojosi nesilaikydama mokėjimo priemonės išdavimą ir naudojimą reglamentuojančių sąlygų ir neįvykdė Mokėjimų įstatymo 34 straipsnyje reglamentuojamų mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigų.

Atsižvelgiant į visas ginčo byloje nustatytas aplinkybes, galima daryti išvadą, kad pareiškėjos veiksmai, dėl kurių ji prarado mokėjimo priemonę, pasireiškė dideliu neatsargumu, tai galiausiai ir lėmė, kad buvo įvykdytos neautorizuotos mokėjimo operacijos iš pareiškėjos sąskaitos ir pareiškėja patyrė nuostolių. Lietuvos banko nuomone, įvertinus pirmiau išdėstytas ginčo byloje nustatytas aplinkybes ir padarytas išvadas, galima teigti, kad pareiškėja iki mokėjimo operacijų įvykdymo galėjo pastebėti, kad jos mokėjimo priemonę pasisavino tretieji asmenys. Mokėjimų įstatymo 39 straipsnio 3 dalyje nustatyta, kad mokėtojai 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.

Vertinant Mokėjimų įstatymo nuostatas, reglamentuojančias atsakomybės už neautorizuotų mokėjimo operacijų įvykdymą pasiskirstymą, tam, kad bankas būtų atleistas nuo pareigos gražinti neautorizuotų mokėjimo operacijų lėšas, turėtų būti nustatytas pareiškėjos sukčiavimas arba didelis neatsargumas. Kaip ir buvo minėta, Lietuvos banko nuomone, nagrinėjamo ginčo atveju pareiškėjos elgesys, dėl kurio ji prarado savo mokėjimo priemonę, gali būti laikomas labai neatsargiu, tai iš esmės ir lėmė neautorizuotų mokėjimo operacijų iš pareiškėjos sąskaitos įvykdymą. Įvertinus pirmiau išdėstytą informaciją, konstatuotina, kad yra pagrindas pareiškėjai taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, todėl pareiškėjos reikalavimas bankui gražinti neautorizuotų mokėjimo operacijų lėšų sumą yra nepagrįstas ir atmestinas.

Dėl mokėjimo operacijų įvykdymo pagrįstumo ir mokėjimo nurodymų įvykdyti mokėjimo operacijas atšaukimo

Pareiškėja teigė, kad bankas turėjo nevykdyti ir atšaukti mokėjimo operacijas, nes kalbėdama su banko darbuotoju ji banką informavo, jog mokėjimo operacijų pati neinicijavo, ir pokalbio metu mokėjimo operacijų lėšos pareiškėjos banko sąskaitoje dar buvo tik rezervuotos.

Vertinant banko pareigos atšaukti mokėjimo operacijas vykdymą, pažymėtina, kad, pagal Mokėjimų įstatymo 44 straipsnio 1 dalies nuostatas, 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).

Remiantis ginčo byloje esančiais duomenimis, pažymėtina, kad pareiškėjos prašymas atšaukti mokėjimo operacijas bankui buvo pateiktas po to, kai mokėjimo nurodymus jau buvo gavęs bankas, todėl Mokėjimų įstatyme nustatytas mokėjimo nurodymo atšaukimo terminas jau buvo praėjęs ir bankas atšaukti pareiškėjos vardu pateiktų mokėjimo nurodymų nebegalėjo. Bankas paaiškino, kad mokėjimo operacijas būtų galėjęs atšaukti tik tuo atveju, jeigu lėšų gavėjai per 9 dienas nebūtų patvirtinę lėšų nurašymo. Tačiau nagrinėjamo ginčo atveju lėšų gavėjai bankui patvirtino lėšų nuskaitymą iš pareiškėjos banko sąskaitos, todėl bankas, nesant lėšų gavėjų sutikimo atšaukti mokėjimo operacijas, jų atšaukti neturėjo galimybes.

Atsižvelgiant į tai, kas buvo išdėstyta pirmiau, nėra pagrindo vertinti, kad bankas nepagrįstai įvykdė mokėjimo operacijas ir kad nepagrįstai jų neatšaukė.

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 arba kitą ginčų nagrinėjimo instituciją įstatymų nustatyta tvarka. Kreipimasis į teismą po Lietuvos banko sprendimo dėl ginčo esmės priėmimo nelaikomas šio Lietuvos banko sprendimo apskundimu. Ginčo šalys turi pareigą pranešti Lietuvos bankui, jeigu viena iš ginčo šalių pareiškia ieškinį bendrosios kompetencijos teismui, prašydama nagrinėti tapatų ginčą iš esmės.

Direktorius

Arūnas Raišutis