



**LIETUVOS BANKO
TEISĖS IR LICENCIJAVIMO DEPARTAMENTO
DIREKTORIUS**

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

2023-09-06 Nr. 429-463
Vilnius

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

N u s t a t y t a:

2023 m. birželio 13 d. iš pareiškėjos sąskaitos banke pareiškėjai banko išduota mokėjimo kortele buvo inicijuotos 5 mokėjimo operacijos gavėjams *Monobank Kyiv UA* bei *Easy Pay Mobile Kyiv UA* (toliau – gavėjai). Bendra mokėjimo operacijų suma – 2 438,21 Eur (toliau – mokėjimo operacijos). Mokėjimo operacijos buvo įvykdytos po to, kai pareiškėja vykdydama trečiųjų asmenų nurodymus paspaudė jai atsiųstą aktyvią nuorodą ir atidarytame neva *Omniva LT* puslapyje, tikėdamasi už parduodamą prekę gauti pinigines lėšas į savo sąskaitą, suvedė savo mokėjimo kortelės duomenis, šiuos duomenis nusavino tretieji asmenys ir inicijavo mokėjimo operacijas, kurias pareiškėja patvirtino savo mobiliajame telefone suvesdama mobiliojo parašo sPIN1 kodą.

Bankui atsisakius pareiškėjai gražinti mokėjimo operacijų sumą, pareiškėja kreipėsi į Lietuvos banką prašydama išnagrinėti vartojimo ginčą ir įpareigoti banką gražinti visą mokėjimo operacijų sumą. Pareiškėja paaiškino, kad „pardavinėjant daiktą, būsimas pirkėjas pasinaudojęs sukčiavimo metodais atsiuntė nuorodą, kurioje kaip teigė reikia patvirtinti identifikaciją, kad galėtų pervesti man pinigus už parduodamą prekę ir užsakyti kurjerį patvirtinant adresą. Paspaudus nuorodą identifikacija patvirtinta nebuvo, tačiau nuo mano kortelės nuskaitytos pinigų sumos <...>“ Pareiškėja teigė, kad buvo suvestas tik mobiliojo parašo sPIN1, o sPIN2 nebuvo įvestas, taip pat paaiškino, kad prieš vedant sPIN1 nebuvo ir informacijos apie tai, kad bus nuskaičiuoti pinigai. Pareiškėjos nuomone, bankas galėjo nevykdyti mokėjimo operacijų, nes kai pareiškėja kreipėsi į banką dėl lėšų iš jos banko sąskaitos vagystės, lėšos pareiškėjos banko sąskaitoje buvo dar tik rezervuotos. Pareiškėja prašė, kad bankas jai gražintų mokėjimo operacijų sumą.

Bankas Lietuvos bankui pateiktame atsiliepime paaiškino, kad pareiškėja dėl savo didelio neatsargumo neišsaugojo savo personalizuotų saugos duomenų, todėl tretieji asmenys jais galėjo pasinaudoti ir be pareiškėjos žinios inicijuoti mokėjimo operacijas. Banko teigimu, mokėjimo operacijos buvo įvykdytos taikant saugesnio autentiškumo patvirtinimo procedūrą – buvo suvesti pareiškėjos mokėjimo kortelės duomenys, žinomi tik kortelės turėtojui: vardas, pavardė, kortelės numeris, galiojimo data ir saugos kodas (CVV), o mokėjimo operacijos patvirtintos suvedant pareiškėjos naudojamos tapatybės atpažinties priemonės mobiliojo parašo sPIN1 kodą. Be to, bankas atkreipė dėmesį ir į tai, kad norint gauti lėšas į savo sąskaitą nereikia suvesti savo mokėjimo kortelės duomenų ir patvirtinti savo tapatybės.

Papildomai bankas atkreipė dėmesį, kad bankas teikia informaciją savo klientams apie tokio pobūdžio sukčiavimo atakas ir ragina būti atsargius, nespauti trečiųjų asmenų pateiktų aktyvių nuorodų ir nevesti savo mokėjimo kortelės duomenų. Banko nuomone, pareiškėja galėjo pastebėti prieš ją vykdomą sukčiavimo ataką ir turėjo susilaikyti nuo tolimesnių veiksmų, tačiau to nepadarė. Banko teigimu, kadangi mokėjimo operacijos buvo tinkamai autorizuotos, bankas mokėjimo operacijas įvykdė pagrįstai.

Pasisakydamas dėl pareiškėjos argumentų, kad, pareiškėjai kreipusis į banką, mokėjimo operacijos nebuvo atšauktos, bankas paaiškino, kad galimybių atšaukti banko ir pareiškėjos

sutartu būdu patvirtintų mokėjimo operacijų po to, kai bankas gavo mokėjimo nurodymus, nebuvo. Kad mokėjimo operacijos būtų atšauktos, būtinas lėšų gavėjo sutikimas, taigi, bankas savo iniciatyva negali atšaukti mokėjimo operacijų ir iš pareiškėjos banko sąskaitos panaikinti lėšų rezervacijos.

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 gražinti pareiškėjai pareiškėjos vardu banke atidarytoje sąskaitoje kortele atliktų mokėjimo operacijų lėšas, iš viso 2 438,21 Eur.

Pareiškėja teigia neautorizavusi (nenorėjusi įvykdyti) mokėjimo operacijų, tačiau ir neneigia trečiųjų asmenų suklastotame *Omniva LT* interneto puslapyje pati suvedusi savo mokėjimo kortelės duomenis, suvedusi savo mobiliojo parašo sPIN1 kodą ir taip patvirtinusi konkrečių mokėjimo operacijų vykdymą. Pareiškėjos teigimu, tuo metu, kai ji kreipėsi į banką ir prašė atšaukti mokėjimo operacijas, mokėjimo operacijų lėšos pareiškėjos sąskaitoje buvo dar tik rezervuotos, todėl bankas galėjo atšaukti mokėjimo operacijų vykdymą ir gražinti pareiškėjai mokėjimo operacijų lėšas. Pareiškėja taip pat teigia, kad prieš ją buvo įvykdyta nusikalstama veika, todėl pati pareiškėja negali būti atsakinga už mokėjimo operacijų įvykdymą ir bankas jai turi gražinti mokėjimo operacijų lėšas.

Bankas teigia, kad mokėjimo operacijos pareiškėjos 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 įvykdytų mokėjimo operacijų. Dėl šių priežasčių, banko nuomone, visi mokėjimo operacijų nuostoliai turėtų tekti pareiškėjai.

Siekdamas išspręsti tarp šalių kilusį ginčą ir įvertinti pareiškėjos bankui keliamą reikalavimą pagrįstumą, Lietuvos bankas vertins, ar: 1) mokėjimo operacijos laikytinos autorizuotomis; 2) bankas turi pareigą gražinti ir (ar) kompensuoti pareiškėjai mokėjimo operacijų sumą; 3) 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.

1. Dėl mokėjimo operacijų autorizavimo

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

Mokėjimų įstatyme nėra nustatytų konkrečių mokėtojo sutikimo įvykdyti mokėjimo operaciją būdų ir (arba) detalios tokio sutikimo davimo tvarkos. Vadovaujantis Mokėjimų įstatymo 13 straipsnio 3 dalies 3 punktu ir 29 straipsnio 1 punktu, mokėtojo sutikimo įvykdyti mokėjimo operaciją davimo sąlygos ir tvarka turi būti aptartos mokėtojo ir mokėjimo paslaugų teikėjo sudaromoje bendrojoje mokėjimo paslaugų teikimo sutartyje (toliau – bendroji sutartis).

Banko mokėjimo paslaugų teikimo sąlygų (toliau – Sąlygos) 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 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 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 priglaidimas 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.“

Nors pirmiau aptartomis banko mokėjimo paslaugų teikimo sąlygų nuostatomis taip pat remiasi bankas, grįsdamas teiginį, kad mokėjimo operacijos buvo tinkamai, t. y. šalių sutartu būdu, autorizuotos, būtina pažymėti, kad minėtose nuostatose kalbama apie atvejus, kai pats mokėtojas duoda savo sutikimą pervesti lėšas ir tuo tikslu panaudoja jam išduotas mokėjimo ir tapatybės patvirtinimo priemones. Vis dėlto nagrinėjamo ginčo atveju, priešingai, nei nurodyta aptariamose nuostatose, pareiškėja savo mokėjimo kortelės personalizuotus saugumo duomenis panaudojo fiktyvioje – atsiradusioje paspaudus elektroniniu paštu gautą nuorodą, interneto svetainėje ir juos suvedė ne dėl to, kad ketino pervesti lėšas, siekdama atsiskaityti už suteiktas paslaugas ar įsigytas prekes, o vykdydama gautoje žinutėje pateiktus nurodymus ir siekdama patvirtinti lėšų gavimą į banke esančią ir su mokėjimo kortele susietą savo sąskaitą. Pareiškėja tiek bendraudama su banku dėl mokėjimo operacijų, tiek kreipimėsi į Lietuvos banką nuosekliai laikosi pozicijos, kad valios inicijuoti ir įvykdyti mokėjimo operacijų ji neišreiškė ir nedavė tam savo sutikimo.

Bankas kartu su atsiliepimu pateikė jo vidaus sistemose užfiksuotus duomenis, pagrindžiančius, kad inicijuojant mokėjimo operacijas buvo suvesti mokėjimo kortelės duomenys (tarp jų ir CVV kodas) ir mokėjimo operacijos papildomai patvirtintos identifikuojant mokėjimo kortelės turėtoją (šiuo atveju – pareiškėja) jo pasirinktu autentifikavimo metodu, t. y. suvedus tik pareiškėjai žinomą jos naudojamos tapatybės patvirtinimo priemonės mobiliojo parašo sPIN1 kodą.

Taigi, bankas, darydamas išvadą, kad mokėjimo operacijos buvo autorizuotos šalių sutarta tvarka, iš esmės remiasi tik tuo faktu, kad, banko vidinės sistemos duomenimis, mokėjimo operacijoms įvykdyti buvo panaudoti mokėjimo kortelės duomenys ir suvestas pareiškėjos mobiliojo parašo sPIN1 kodas, tačiau, darydamas tokią išvadą, bankas nevertino, kada, kaip ir kas perdavė lėšų gavėjui ir (arba) jo mokėjimo paslaugų teikėjui duomenis, kurių pagrindu buvo inicijuotos mokėjimo operacijos, t. y. ar šiuos duomenis tiesiogiai pateikė pati pareiškėja, ar iš pareiškėjos šiuos duomenis neteisėtai išvilioję tretieji asmenys.

Lietuvos banko vertinimu, vien pirmiau minėti duomenys dar savaime neįrodo, kad mokėjimo operacijos iš tiesų atliktos gavus pareiškėjos sutikimą. Vadovaujantis Mokėjimų įstatymo nuostatomis, vien aplinkybė, kad mokėtojo mokėjimo paslaugų teikėjo vidaus sistemose užregistruotas mokėtojai išduotos mokėjimo priemonės, įskaitant jos personalizuotus saugumo duomenis, naudojimas, nebūtinai yra pakankamas įrodymas, kad mokėjimo priemone naudojosi ir (arba) mokėjimo operaciją autorizavo pats mokėtojas (Mokėjimų įstatymo 37 straipsnio 3 dalis).

Bankas, pagrįsdamas savo poziciją, kad mokėjimo operacijos buvo tinkamai autorizuotos, be kita ko, nurodo, kad, identifikacijai pasirinkus mobilųjį parašą, mokėjimo kortelės savininkas yra nustatomas pagal šios tapatybės patvirtinimo priemonės paskyros sPIN1 kodą. Tokiais atvejais mobiliajame telefone yra rodomas operacijos kontrolinis kodas, kuris turi sutapti su kontroliniu kodu, kurį mokėtojas mato banko autentifikavimo lange. Bankas paaiškino, kad jo 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 – prieš suveddamas savo mobiliojo parašo SPIN1 kodą, turi įsitikinti, kad mokėjimo operacijos lange rodomas kontrolinis kodas sutampa su mobiliajame telefone rodomu kontroliniu kodu, o jeigu tokios galimybės neturi, neautorizuoti atliekamo veiksmo.

Vis dėlto, remiantis banko paaiškinimais, be kontrolinio kodo, kurį turi sutikrinti mokėtojas, tvirtindamas per gavėją inicijuotą mokėjimo operaciją, nėra atliekami jokie kiti veiksmai ir mokėtojui, be banko interneto banke operacijos lange nurodytų duomenų, papildomai nėra rodoma jokia informacija, susijusi su inicijuota mokėjimo operacija.

Būtina atkreipti dėmesį ir į tai, kad, nustatytais duomenimis, mokėjimo operacijoms inicijuoti būtini duomenys buvo suvesti suklastotoje interneto svetainėje, kurioje pareiškėjai buvo rodoma informacija apie siekiamą iš jos įsigyti prekę ir buvo prašoma pateikti duomenis tariamam lėšų įskaitymui į sąskaitą. Dėl šios priežasties ginčo byloje nėra jokių duomenų, kurie galėtų patvirtinti, kad pareiškėja, duomenis, būtinus mokėjimo operacijai inicijuoti, suvedusi suklastotoje interneto svetainėje, turėjo ir galėjo matyti ir tokio tipo operacijas per gavėją inicijavusiems klientams interneto banke įprastai rodomą operacijos aprašymo langą, kuriame ir rodoma pirmiau minėta informacija apie mokėtojo inicijuotą mokėjimą, t. y. gavėjas, suma, mokėjimo kortelės paskutiniai 4 skaitmenys ir kontrolinis kodas, kurį reikia sutikrinti su mobiliojo telefono lange matomu kontroliniu kodu. Ši aplinkybė ypač svarbi ir dėl to, kad šalių sutartinius santykius reguliuojančiuose dokumentuose nėra paaiškinama, nurodoma mobiliojo parašo, kaip tapatybės patvirtinimo priemonės, SPIN1 kodo suvedimo reikšmė mokėjimo operacijų vykdymo procese.¹

Vadinasi, ginčo byloje esantys įrodymai, tarp jų ir pirmiau aptarti duomenys dėl mokėjimo operacijų inicijavimo ir įvykdymo aplinkybių, kurių nepaneigė banko paaiškinimai ir pateikti vidinės sistemos duomenys, kad mokėjimo operacijoms patvirtinti panaudoti pareiškėjos mokėjimo kortelės duomenys ir suvestas pareiškėjos mobiliojo parašo sPIN1 kodas, Lietuvos banko vertinimu, leidžia pagrįstai daryti išvadą, kad trečiųjų asmenų sukurtoje aplinkoje pareiškėjai apie prašymą atskleisti mokėjimo kortelės personalizuotus saugumo duomenis, būtinus mokėjimo operacijai kortele inicijuoti, buvo rodoma tikrovės neatitinkanti informacija, kuri galėjo suklaidinti pareiškėją dėl prašomų atlikti veiksmų (atskleidžiamos konfidencialios informacijos) esmės ir pobūdžio. Vadinasi, duomenų, kad pareiškėja žinojo, suprato ir išreiškė savo valią inicijuoti ir autorizuoti mokėjimo operacijas šalių sutarta tvarka, ginčo byloje nėra.

Atsižvelgiant į tai, Lietuvos banko nuomone, vertinti mokėjimo operacijas kaip autorizuotas – atliktas esant pačios pareiškėjos sutikimui (kaip tai suprantama Mokėjimų įstatymo 29 straipsnio 1 dalies kontekste), nors jos ir atitiko pareiškėjos ir banko sutartą sutikimo atlikti mokėjimo operacijas davimo formą ir tvarką, nėra pagrindo, todėl Lietuvos bankas daro išvadą, kad mokėjimo operacijos laikytinos neautorizuotomis.

2. Dėl neautorizuotų mokėjimo operacijų pasekmių ir pareiškėjos teisės į mokėjimo operacijų sumų gražinimą

Vadovaudamasis Mokėjimų įstatymo 38 straipsnio 1 dalimi, 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 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

¹ Apie tapatybės patvirtinimo priemonės PIN kodų suvedimo svarbą Lietuvos bankas ne kartą yra plačiau pasisakęs savo ginčų nagrinėjimo praktikoje, pavyzdžiui, ginčo byla Nr. [2022-03143](#), ginčo byla Nr. [2022-02907](#).

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 didžiausios 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 suponuoją 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 nustatytų mokėtojo pareigų ir neužtikrino, kad, be pareiškėjos, turinčios teisę naudotis mokėjimo priemone, personalizuotais saugumo duomenimis negalėtų pasinaudoti kiti asmenys.

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 paspaudė trečiųjų asmenų jai per *Messenger* programėlę atsiųstą aktyvią nuorodą, pateko į neva tikrąjį *Omniva LT* puslapį, jame suvedė savo mokėjimo kortelės duomenis, o vėliau savo mobiliajame telefone kelis kartus suvedė savo mobiliojo parašo SPIN1 kodą ir taip patvirtino mokėjimo operacijų gavėjui vykdymą.

Iš pareiškėjos pateiktų paaiškinimų matyti, kad, spausdama trečiųjų asmenų jai atsiųstoje žinutėje pateiktą aktyvią nuorodą, patekusi neva į *Omniva LT* puslapį ir jame vesdama savo kortelės duomenis, pareiškėja tikėjosi už prekę gauti pinigus į savo sąskaitą banke.

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, pareiškėja savo mokėjimo priemonę naudojo ne pagal sutartyje su pareiškėja sutartą mokėjimo priemonės naudojimo paskirtį, nes norint gauti lėšas į savo sąskaitą nereikia suvesti savo mokėjimo kortelės duomenų ir juo labiau lėšų gavimo patvirtini suvedant mobiliojo parašo SPIN1 kodą.

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 tuo susijusių aplinkybių konteksto.

Kriterijai, į kuriuos reikėtų atsižvelgti vertinant kaltės laipsnį, yra iš dalies suformuluoti Antrosios mokėjimo paslaugų direktyvos (toliau – PSD2) 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“².

Vertinant, ar pareiškėjos elgesys, kai ji paspaudė trečiųjų asmenų atsiųstoje žinutėje

Commented [RC1]: Kažkur aukščiau buvo nurodyta, kad el. paštu gautą nuorodą.

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

esančią aktyvią nuorodą norėdama gauti pinigines lėšas į savo banko sąskaitą, suvedė savo mokėjimo kortelės duomenis bei savo mobiliajame telefone suvedė mobiliojo parašo SPIN1 kodą, gali būti vertinamas kaip labai neatsargus, t. y. toks elgesys, dėl kurio mokėjimo priemonės turėtojo veiksmai iš esmės skiriasi nuo atsargaus elgesio reikalavimų, pažymėtina, kad įprastai panašaus pobūdžio ginčo bylose Lietuvos bankas vertina, kad vien tik faktas, kad mokėtojas paspaudžia jam trečiųjų asmenų atsiųstą aktyvią nuorodą ir nepastebi, kad patenka į suklastotą kokios nors bendrovės interneto puslapį, savaime nereiškia mokėtojo didelio neatsargumo. Paprastai sukčių pateiktos tiek pačios nuorodos į suklastotas bendrovių interneto svetaines, tiek ir pačios svetainės būna parengtos labai profesionaliai, dėl to vidutiniam vartotojui pagrįstai gali atrodyti, kad jis jungiasi prie tikros kokios nors bendrovės interneto svetainės.

Nagrinėjamos ginčo atveju matyti, kad trečiųjų asmenų pareiškėjai atsiųsta nuoroda <https://omniva.lt-info.sunkvezimiais.com/cash66921248> buvo klaidinga ir nepanaši į galinčią atrodyti teisingą prisijungimo prie tikros bendrovės *Omniva LT* interneto svetainės nuorodą. Bendrovės skelbiami oficialūs interneto svetainės adresai yra tik du: www.omniva.lt, www.mano.omniva.lt. Lietuvos banko nuomone, pareiškėjai pateikta aktyvi nuoroda buvo pakankamai akivaizdžiai klaidinga, kad pareiškėjai sukeltų bent minimalias dvejetas dėl jos tikrumo ir sustabdytų nuo tolimesnių veiksmų su savo mokėjimo priemone atlikimo.

Taip pat svarbu pažymėti, kad panašaus pobūdžio sukčiavimo atakos nėra naujos ir visuomenėje yra gana plačiai žinomos, nes periodiškai yra skelbiama nemažai viešai prieinamos informacijos, įspėjančios vartotojus apie panašias sukčiavimo atakas ir raginančios vartotojus būti budrius, nespauti aktyvių nuorodų ir nevesti savo mokėjimo kortelės bei kitų personalizuotų saugos duomenų. Atsižvelgiant į pirmiau minėtą informaciją, galima teigti, kad pareiškėja galėjo pastebėti, kad jai pateikta nuoroda yra įtartina, ir galėjo susilaikyti nuo tolimesnių veiksmų bei imtis veiksmų, kad įsitikintų jai pateiktos nuorodos tikrumu.

Vertinant tolimesnius pareiškėjos veiksmus pareiškėjai paspaudus aktyvią nuorodą ir patekus į trečiųjų asmenų suklastotą *Omniva LT* puslapį, pažymėtina, kad, kaip nurodė pareiškėja, ji 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 mokėjimo operaciją. Tačiau būtent siekdama už prekę gauti pinigų į savo banko sąskaitą pareiškėja suvedė savo mokėjimo kortelės duomenis ir pavirtino lėšų įskaitymą į banko sąskaitą. Taigi, tam, kad pareiškėja 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.

Kad pinigines lėšas būtų gautos į banko sąskaitą, bankai neprašo sąskaitos turėtojo pateikti savo mokėjimo kortelės duomenų ir neprašo suvesti mobiliojo parašo SPIN 1 kodo. Pareiškėjai faktas, kad norėdama į savo sąskaitą gauti pinigines lėšas ji turėjo suvesti duomenis, kurie iš esmės yra reikalingi atlikti priešingą veiksmą – patvirtinti lėšų iš banko sąskaitos nurašymą, nesukėlė įtarimų ir pareiškėja vykdė trečiųjų asmenų nurodymus. Taigi, pareiškėja, nors ir turėjo galimybę kritiškai įvertinti savo veiksmų su mokėjimo priemone riziką ir galimas pasekmes, nuo tolimesnių veiksmų nesusilaikė, o priešingai, vykdė trečiųjų asmenų nurodymus ir netgi keletą kartų suvedė savo mobiliojo parašo SPIN1 kodą.

Kaip minėta, Sąlygų 6.3.1 papunktyje aiškiai reglamentuota, kad banko klientui suteiktų personalizuotų duomenų naudojimas yra skirtas duoti sutikimą įvykdyti mokėjimo operaciją. Ginčo byloje nėra duomenų, 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 mobiliojo parašo SPIN1 kodo 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 kritiška savo su mokėjimo priemone atliekamų veiksmų atžvilgiu ir būtų susilaikiusi nuo veiksmų su savo mokėjimo priemone, ji būtų galėjusi išvengti neautorizuotų mokėjimo operacijų iš savo sąskaitos įvykdymo. Nagrinėjamu atveju pareiškėja turėjo galimybę suprasti, 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 yra atliekami norint įvykdyti mokėjimo operacijas iš banko sąskaitos. Pareiškėja turėjo kritiškai įvertinti trečiųjų asmenų jai atsiųstą nuorodą ir prašomus atlikti veiksmus su savo mokėjimo priemone. Tačiau pareiškėja fakto, kad jos buvo prašoma suvesti mobiliojo parašo SPIN1 kodą, nors ji pati ir nesiekė inicijuoti jokių mokėjimo operacijų, kurioms patvirtinti reikia suvesti personalizuotus saugos duomenis,

o tik siekė gauti lėšas į savo sąskaitą, nors lėšoms įskaityti į sąskaitą nereikia suvesti savo personalizuotų saugos duomenų, nevertino kritiškai ir vykdė trečiųjų asmenų jai pateiktus nurodymus. Lietuvos banko vertinimu, toks pareiškėjos elgesys gali būti pripažintas kaip elgesys, iš esmės besiskiriantis nuo atsargaus elgesio reikalavimų, tai 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) 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 (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.

Visų ginčo byloje nustatytų aplinkybių kontekste 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.

Mokėjimų įstatymo 39 straipsnio 3 dalyje nustatyta, kad mokėtoji 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.

Įvertinus pirmiau išdėstytą informaciją, konstatuotina, kad yra pagrindas pareiškėjai taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, todėl pareiškėjos reikalavimas bankui grąžinti neautorizuotų mokėjimo operacijų lėšų sumą yra nepagrįstas ir atmestinas.

3. Dėl mokėjimo nurodymų įvykdyti mokėjimo operacijas atšaukimo

Pareiškėja teigė, kad bankas turėjo nevykdyti ir atšaukti mokėjimo operacijas, nes pokalbio su banko darbuotoju metu pareiškėja banką informavo, kad 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 grąžinimas mokėtojui, esant jo atitinkamam prašymui (pasibaigus 44 straipsnio 1 dalyje nurodytam terminui).

Remiantis ginčo byloje esančiais duomenimis, 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.

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 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