LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

SPRENDIMAS DĖL X.X. IR AB ŠIAULIŲ BANKO GINČO NAGRINĖJIMO

2023-07-19 Nr. 429-423
Vilnius

Lietuvos bankas gavo advokato padėjėjos X.X.(toliau – pareiškėjos atstovė) kreipimąsi, kuriuo prašoma išnagrinėti tarp X.X. (toliau – pareiškėja) ir AB Šiaulių banko (toliau – bankas), kilusį ginčą.

N u s t a t y t a:

2023 m. vasario 21 d. iš pareiškėjos sąskaitos banke buvo inicijuota 18 000 Eur mokėjimo operacija (toliau – mokėjimo operacija) gavėjui *Hugo alexandre goncalves dos reis* (toliau – gavėjas).

Bankui atsisakius pareiškėjai grąžinti pareiškėjos neautorizuotos mokėjimo operacijos sumą, pareiškėja kreipėsi į Lietuvos banką prašydama išnagrinėti vartojimo ginčą ir įpareigoti banką grąžinti neautorizuotos mokėjimo operacijos sumą – 17 950 Eur.

Kreipimesi į Lietuvos banką pareiškėjos atstovė paaiškino, kad pareiškėja „savo mobiliojo telefono *Google Chrome* naršyklės laukelyje surinko raktinius žodžius „siauliu bankas". Ekrane pasirodė išreitinguotos nuorodos patekti į banko internetinį puslapį. Pareiškėja pasirinko pirmąją nuorodą. Ši nuoroda nesukėlė jokių įtarimų ir, normalu, kad tai sumažino Pareiškėjos budrumą. Internetinis puslapis buvo identiškas įprastam Banko internetiniam puslapiui – laukelių vietos, prisijungimo duomenų poreikis (vartotojo ID ir slaptažodis), logotipas. Jokio įtarimo, jog tai galėtų būti suklastotas/ fiktyvus puslapis, nebuvo.

Nieko įtartino nepastebėjusi, Pareiškėja jungėsi į savo Banko paskyrą, suvesdama prisijungimo informaciją – vartotojo ID bei slaptažodį. Asmens tapatybės patvirtinimui, kaip įprastai, pasirodė Smart ID programėlė, prašydama suvesti pirmąjį PIN kodą – jis buvo suvestas. Puslapis neužsikrovė, seko laiko limitas, todėl Pareiškėja perkrovė Banko internetinį puslapį, tikėdama, kad tai techniniai gedimai, ar interneto trikdžiai, nes Banko internetinis puslapis neretai stringa. Perkrovus internetinį puslapį, buvo vėl grįžta į pradinį puslapį. Prisijungimui naujai buvo suvesti tie patys duomenys bei patvirtinimas pirmuoju PIN kodu Smart ID programėlėje. Situacija nesikeitė, puslapis strigo, neįleido į paskyrą – buvo vėl perkrautas puslapis.

Tokia pati situacija kartojosi apie 5 kartus. Paskutinio bandymo metu pasirodė Smart ID programėlė, prašydama patvirtinti 18 000 Eur likutį, surenkant antrąjį PIN kodą, kurį Pareiškėja, nieko neįtardama, suvedė. Dėl techninių trikdžių prieš tai buvusiais atvejais buvo paprašyta patvirtini tapatybę, asmens kodą. Manydama, kad to prašoma dėl prieš tai paminėtos priežasties ar galimo bandymo įsilaužti į Pareiškėjos paskyrą iš išorės, ji pasielgė kaip įprastai, t. y. suvedė antrąjį PIN kodą Smart ID programėlėje. Po šio veiksmo Pareiškėjos į jos paskyrą vis tiek neįleido."

Pareiškėjos atstovė teigė, kad po to, kai nepavyko prisijungti prie interneto banko paskyros, pareiškėja tame pačiame mobiliajame įrenginyje, tik jau per kitą interneto naršyklę, suvedė tuos pačius banko raktinius žodžius „siauliu bankas", pasirinko pirmąją internetinę nuorodą, pateko į banko interneto puslapį ir pakartojo visus prisijungimo prie interneto banko paskyros veiksmus. Tuomet pareiškėja ir pamatė, kad jos banko sąskaitoje liko tik 377,49 Eur.

Pareiškėjos atstovės teigimu, bankui turėjo kilti įtarimų tiek ir dėl didelės mokėjimo operacijos sumos, tiek ir dėl neaiškaus lėšų gavėjo. Pareiškėjos atstovė paaiškino, kad pareiškėja iš savo banko sąskaitos labai retai atlikdavo mokėjimo operacijas ir ne tokiomis didelėmis sumomis. Pareiškėjos atstovės teigimu, turėjo suveikti banko mokėjimo operacijų

kontrolės sistema, bankas turėjo sustabdyti mokėjimo operaciją ir jos nevykdyti ir kreiptis į pareiškėją.

Pareiškėjos atstovė teigė, kad bankas įvykdydamas mokėjimo operaciją pažeidė Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymo (toliau – PPTFPĮ) 9 straipsnio 1 straipsnio 2 punktą, nes nesiėmė jokių priemonių įsitinkinti piniginės operacijos tikrumu ir legalumu ir netikrino gavėjo asmens tapatybės. Bankui piniginė operacija nesukėlė jokio įtarimo ir bankas nesiaiškino, kaip fizinis asmuo iš savo banko sąskaitos vienu momentiniu pavedimu perveda 18 000 Eur į neaiškaus asmens sąskaitą Ispanijoje su neaiškia mokėjimo paskirtimi. Pareiškėjos atstovės teigimu, bankas elgėsi neatsakingai, neapdairiai ir būtent dėl banko kaltės pareiškėja prarado jai priklausančią pinigų sumą.

Pareiškėjos atstovės teigimu, mokėjimo operacija buvo įvykdyta be pareiškėjos žinios ir sutikimo, todėl turėtų būti laikoma neautorizuota, o bankas turėtų pareiškėjai grąžinti įvykdytos neautorizuotos mokėjimo operacijos sumą. Pareiškėjos atstovė nesutinka su banko pozicija, kad pareiškėja naudodama savo personalizuotus saugos duomenis elgėsi itin aplaidžiai, ir teigia, kad bankas neįrodė, jog pareiškėjos veiksmai su savo mokėjimo priemone buvo labai aplaidūs ir dėl to visi neautorizuotos mokėjimo operacijos nuostoliai turėtų tekti pareiškėjai.

Pareiškėjos atstovė prašė taikyti Lietuvos Respublikos mokėjimų įstatymo 39 straipsnio 1 dalį, kurioje nustatyta, kad 50 Eur dėl neautorizuotos mokėjimo operacijos nuostolių tenka mokėtojui, o likusi suma bankui, ir įpareigoti banką kompensuoti pareiškėjai 17 950 Eur 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 operaciją. Bankas paaiškino, kad pareiškėjai, kaip ji pati teigė, prašymas daugiau nei 5 kartus patvirtinti savo tapatybę ir taip prisijungti prie banko sąskaitos suvedant „Smart-ID" PIN1 kodą pasirodė įtartinas, tačiau ji nesiėmė jokių saugumo priemonių ir toliau vedė savo personalizuotus saugos duomenis. Banko teigimu, tikėtina, kad pareiškėja, tvirtindama mokėjimo operaciją suvesdama „Smart-ID" PIN2 kodą, neperskaitė „Smart-ID" programėlės ekrane rodomo teksto „18 000 EUR i saskaita ***2217. Patvirt'-", informavusio pareiškėją, kokiu tikslu jos prašoma suvesti šį kodą, ir neapdairiai patvirtino mokėjimo operaciją.

Bankas teigia dedantis visas įmanomas pastangas informuoti savo klientus apie galimus sukčiavimo atvejus. Banko mobiliojoje programėlėje ir interneto svetainėje banko klientai yra nuolat supažindinami su naujais sukčiavimo atvejais ir nuo jų apsaugančiomis prevencinėmis priemonėmis. Socialinėje erdvėje, banko *Facebook* profilyje, klientai ne tik yra informuojami apie banko nustatytus sukčiavimo atvejus, bet ir tarpusavyje dalijasi patirtimi.

Pasisakydamas dėl pareiškėjos atstovės teiginio, kad pareiškėja nebuvo tinkamai supažindinta su „Smart-ID" programėlės naudojimo ir PIN kodų suvedimo reikšme, bankas teigė, kad pareiškėja banko interneto banko paslaugomis naudojasi nuo 2016 metų, todėl naudojimosi „Smart-ID" programėle esminiai ypatumai (pavyzdžiui, kokiu tikslu gali būti prašoma suvesti „Smart-ID" PIN2 kodą) pareiškėjai turėjo būti žinomi. Bankas taip pat atkreipė dėmesį į tai, kad niekada neprašo klientų patvirtinti banko sąskaitoje esančių piniginių lėšų likučio. Pareiškėja pati pasirinko „Smart-ID" tapatybės nustatymo būdą, todėl pačiai pareiškėjai ir atsirado pareiga susipažinti su programėlės naudojimosi instrukcija. Be to, klientai su „Smart-ID" naudojimosi instrukcijomis yra supažindinami ne tik programėlės kūrėjų, bet ir banko interneto svetainėje.

Taigi, banko teigimu, pareiškėja kritiškai neįvertino interneto naršyklėje atsiradusios nuorodos, neįsitikino interneto svetainės saugumu ir suklastotoje interneto banko svetainėje suvedė savo personalizuotus saugumo duomenis. Pareiškėja nedvejojusi suvedė savo „Smart-ID" paskyros PIN2 kodą tik todėl, kad nebuvo atsargi ir rūpestinga, kiek akivaizdžiai buvo būtina vertinamomis aplinkybėmis. Pareiškėjos elgesys vertinamomis aplinkybėmis nebuvo toks, koks akivaizdžiai buvo būtinas, ir tai šiuo atveju lėmė, kad tretieji asmenys įgijo galimybę pareiškėjos vardu inicijuoti mokėjimo operaciją, suvesdama savo „Smart-ID" paskyros PIN2 kodą pati pareiškėja patvirtino šią mokėjimo operaciją, prieš tai neperskaičiusi ir (ar) neįvertinusi „Smart-ID" programėlės pranešimo, taigi, nesudvejojusi dėl tokio prašymo naudoti savo atpažinties priemonę pagrįstumo. Banko teigimu, visi dėl neautorizuotos mokėjimo operacijos atsiradę nuostoliai turi tekti pačiai pareiškėjai.

Pasisakydamas dėl pareiškėjos atstovės argumentų, kad bankas prieš įvykdydamas mokėjimo operaciją netikrino gavėjo duomenų, bankas teigė, kad teisės aktai neįpareigoja bankų tikrinti kiekvienos jų klientų atliekamos mokėjimo operacijos, papildomai rinkti ir (arba)

tikrinti duomenis apie kiekvieną mokėjimo nurodyme nurodytą mokėjimo operacijos sumos gavėją, analizuoti lėšų gavėjo vykdomos veiklos specifikos ar kitaip kvestionuoti mokėtojo, kuris pateikė mokėjimo nurodymą pervesti tokiam gavėjui lėšas, veiksmus, jeigu, objektyviai vertinant, nėra pagrindo įtarti, jog mokėtojo atliekamos operacijos gali būti susijusios su pinigų plovimo ar teroristų finansavimo veikla.

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. Lietuvos bankas ginčo nagrinėjimo proceso metu neatlieka Lietuvos Respublikos Lietuvos banko įstatymo 42^1 straipsnyje reglamentuotų patikrinimų, skirtų faktinėms aplinkybėms, susijusioms su Lietuvos banko priežiūrimo finansų rinkos dalyvio galimai padarytu Lietuvos banko kompetencijai priskirtų teisės aktų reikalavimų pažeidimu, nustatyti ir įvertinti. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Pareiškėjos ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjai pareiškėjos vardu banke atidarytoje sąskaitoje atliktos mokėjimo operacijos lėšas, iš viso 17 950 Eur. Pareiškėja teigia neautorizavusi (nenorėjusi įvykdyti) mokėjimo operacijos, tačiau ir neneigia trečiųjų asmenų suklastotame banko interneto puslapyje pati suvedusi savo personalizuotus saugos duomenis, skirtus prisijungti prie banko sąskaitos, ir savo mobiliajame telefone suvedusi „Smart-ID" PIN1 bei PIN2 kodus ir taip patvirtinusi mokėjimo operacijos įvykdymą. Pareiškėjos atstovės teigimu, pareiškėjos elgesys su savo mokėjimo priemone negali būti pripažįstamas labai neatsargiu ir dėl to pareiškėjai turėtų tekti visi su mokėjimo operacija susiję nuostoliai. Priešingai, pareiškėjos atstovė teigia, kad, įvykdydamas mokėjimo operaciją, bankas pažeidė PPTFPĮ reikalavimus, dėl to visa kaltė dėl neautorizuotos mokėjimo operacijos įvykdymo turėtų tekti bankui.

Bankas teigia, kad pareiškėjos mokėjimo operacija buvo patvirtinta šalių sutarta forma ir tvarka, dėl to bankas ją pagrįstai įvykdė. 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 įvykdytos mokėjimo operacijos. Dėl šios priežasties, banko nuomone, visi mokėjimo operacijos nuostoliai turėtų tekti pareiškėjai.

Svarbu pažymėti, kad tarp šalių nėra ginčo, kad nebuvo duotas pareiškėjos sutikimas vykdyti mokėjimo operaciją, t. y. tiek pareiškėjos atstovė, tiek bankas pripažįsta, kad mokėjimo operaciją inicijavo ne pati pareiškėja, o tretieji asmenys, neteisėtu būdu pasisavinę pareiškėjos mokėjimo priemonę. Atsiliepime bankas iš esmės remiasi Mokėjimų įstatymo nuostatomis, reglamentuojančiomis mokėtojo atsakomybę už neautorizuotas mokėjimo operacijas. Taigi, galima daryti išvadą, kad bankas pripažįsta, kad mokėjimo operacija nagrinėjamo ginčo atveju laikytina neautorizuota. Atsižvelgiant į tai, kad iš esmės abi ginčo šalys sutaria, kad mokėjimo operacija galėjo būti inicijuota be pareiškėjos žinios ir sutikimo, toliau sprendime nebus analizuojamos su mokėjimo operacijos autorizavimo vertinimu susijusios aplinkybės, o mokėjimo operacija laikoma pareiškėjos neautorizuota.

Siekdamas išspręsti tarp šalių kilusį ginčą ir įvertinti pareiškėjos bankui keliamo reikalavimo pagrįstumą, Lietuvos bankas vertins, ar: 1) bankas turi pareigą grąžinti ir (ar) kompensuoti pareiškėjai mokėjimo operacijos sumą – 17 950 Eur; 2) bankui kyla civilinė atsakomybė dėl įvykdytos mokėjimo operacijos.

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

1. Dėl neautorizuotos mokėjimo operacijos pasekmių ir pareiškėjos teisės į 17 950 Eur

mokėjimo operacijos sumos grąžinimą

Vadovaujantis 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 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 suponuoja atlikto veiksmo teisinio pagrindo nebuvimą.

Bankas teigia, kad tretieji asmenys neteisėtu būdu galėjo pasisavinti pareiškėjos personalizuotus saugos duomenis ir inicijuoti mokėjimo operaciją, kurios įvykdymą patvirtino pati pareiškėja suvesdama „Smart-ID" PIN kodus, 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 operacijos įvykdymo aplinkybes iš esmės sutampa. Ginčo byloje nustatyta, kad pareiškėja prarado savo mokėjimo priemonę, kai per savo mobiliojo telefono naršyklę surinkusi raktinius banko pavadinimo žodžius „siauliu bankas" mėgino jungtis prie savo interneto banko paskyros, paspaudė aktyvią nuorodą ir pateko į neva tikrąjį banko interneto puslapį, jame suvedė savo banko ID bei prisijungimo slaptažodį ir prisijungimą prie interneto banko patvirtino savo mobiliajame telefone kelis kartus suvesdama „Smart-ID" PIN1 kodą. Vėliau pareiškėja suvedė „Smart-ID" PIN2 kodą ir taip patvirtino mokėjimo operacijos vykdymą.

Iš pareiškėjos atstovės pateiktų paaiškinimų matyti, kad, spausdama trečiųjų asmenų suklastotą banko interneto svetainės adresą, taip patekusi neva į banko puslapį ir jame vesdama savo banko ID ir slaptažodį bei vėliau „Smart-ID" PIN1 kodą, pareiškėja siekė prisijungti prie savo sąskaitos banke. Tačiau vesdama „Smart-ID" PIN2 kodą pareiškėja, kaip teigia pareiškėjos atstovė, nors ir matė „Smart-ID" programėlės lange su mokėjimo pavedimu susijusią informaciją: „18 000 EUR i saskaita ***2217. Patvirt'-", tačiau „Smart-ID" PIN2 kodą vedė manydama, kad jos prašoma patvirtinti lėšų jos sąskaitoje likutį arba mėgindama užkardyti įsilaužimą į jos banko sąskaitą.

Teigdamas, kad pareiškėjos elgesys, dėl kurio ji prarado savo mokėjimo priemonę, turi didelio neatsargumo požymių, bankas remiasi tuo, kad pareiškėja nesilaikė mokėtojui nustatytos pareigos saugoti personalizuotus saugos duomenis ir niekam jų neatskleisti. Taip pat, banko teigimu, pareiškėja savo mokėjimo priemonę naudojo ne pagal sutartyje sutartą mokėjimo priemonės naudojimo paskirtį, nes bankas neprašo suvesti savo personalizuotų saugos duomenų, įskaitant „Smart-ID" PIN1 bei PIN2 kodus, tam, kad būtų patvirtintas lėšų banko sąskaitoje likutis.

Atkreiptinas dėmesys, 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 vykdymo 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"[1].

Vertinant, ar pareiškėjos elgesys, kai ji paspaudė interneto naršyklėje trečiųjų asmenų pateiktą aktyvią nuorodą, norėdama prisijungti prie savo banko sąskaitos, ir suvedė savo banko ID ir slaptažodį bei vėliau savo mobiliajame telefone suvedė „Smart-ID" PIN1 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 trečiųjų asmenų suklastotą aktyvią nuorodą ir nepastebi, kad patenka į suklastotą kokios nors bendrovės interneto puslapį, savaime nereiškia mokėtojo didelio neatsargumo. Paprastai sukčių pateiktos nuorodos į suklastotas bendrovių interneto svetaines, taip pat ir pačios svetainės būna parengtos labai profesionaliai, dėl to vidutiniam vartotojui pagrįstai gali atrodyti, kad jis jungiasi prie tikros kokios nors bendrovės interneto svetainės.

Lietuvos bankui nebuvo pateiktas trečiųjų asmenų suklastotos banko interneto svetainės vaizdas, todėl neturime galimybės įvertinti, ar trečiųjų asmenų suklastota banko interneto svetainė vizualiai galėjo būti panaši į tikrąją banko interneto banko svetainę. Kita vertus, pareiškėjos atstovė Lietuvos bankui pateikė mobiliojo telefono naršyklės naršymo istoriją, iš kurios matyti pareiškėjai trečiųjų asmenų pateikta banko interneto banko svetainės nuoroda *sb.lt.esbankas.online.* Iš viešai prieinamos informacijos matyti, kad tikrosios banko interneto banko svetainės adresas yra – *e.sb.lt.* Palyginus šias dvi nuorodas, galima teigti, kad vizualiai jos gana skirtingos, todėl pareiškėja galėjo pastebėti šį vizualinį skirtumą ir susilaikyti nuo tolimesnių veiksmų.

Vertinant tolimesnius pareiškėjos veiksmus, pareiškėjai paspaudus aktyvią nuorodą ir patekus į trečiųjų asmenų suklastotą banko puslapį, pažymėtina, kad, kaip nurodė pareiškėjos atstovė, pareiškėja turėjusi tikslą prisijungti prie savo banko sąskaitos. Būtent šiuo tikslu pareiškėja ir suvedė savo banko ID, slaptažodį bei „Smart-ID" PIN1 kodą. Pagal banko ir pareiškėjos pateiktus paaiškinimus, pareiškėja net 5 kartus vedė „Smart-ID" PIN1 kodą, tačiau negalėjo prisijungti prie savo banko sąskaitos. Taigi, pareiškėja kritiškai nevertino situacijos, nesusilaikė nuo tolimesnių veiksmų ir vėliau, nors „Smart-ID" paskyroje ir matė (kaip teigia pareiškėjos atstovė) su mokėjimo pavedimu susijusią informaciją „18 000 EUR i saskaita ***2217. Patvirt'-", kritiškai šios informacijos nevertino ir suvedė „Smart-ID" PIN2 kodą, taip patvirtindama 18 000 Eur mokėjimo operacijos vykdymą. Pareiškėjos atstovė teigia, kad pareiškėja vesdama „Smart-ID" PIN2 kodą tikėjosi, kad tvirtina lėšų savo banko sąskaitoje likutį arba užkerta kelią įsilaužimui į sąskaitą.

Vertinant, ar pareiškėja pagrįstai galėjo tikėtis, kad vesdama „Smart-ID" PIN2 kodą tvirtina lėšų savo banko sąskaitoje likutį arba užkerta kelią įsilaužimui į jos sąskaitą, pažymėtina, kad bankai neprašo patvirtinti lėšų banko sąskaitoje likučio ir šiuo tikslu suvesti savo personalizuotų saugos duomenų, įskaitant ir „Smart-ID" PIN kodus. Iš pareiškėjos atstovės pateiktų paaiškinimų, kad pareiškėja vesdama „Smart-ID" PIN2 kodą siekė ne tik patvirtinti lėšų savo sąskaitoje likutį, bet ir užkirsti kelią galimam sukčiavimui, galima daryti prielaidą, kad pareiškėja vis dėlto įtarė, kad prieš ją gali būti vykdoma sukčiavimo ataka, tačiau nuo tolimesnių veiksmų su savo mokėjimo priemone nesusilaikė, o priešingai, net ir matydama su mokėjimo pavedimu susijusią informaciją ir įtardama sukčiavimą, toliau tęsė veiksmus, kuriais galiausiai patvirtino mokėjimo operacijos iš savo banko sąskaitos įvykdymą.

Pareiškėjos atstovė kreipimesi į Lietuvos banką teigė, kad pareiškėja banko nebuvo pasirašytinai supažindinta su „Smart-ID" naudojimo sąlygomis, todėl negalėjo suvokti savo veiksmų pasekmių. Bankas teigia, kad su „SmartID" naudojimosi sąlygomis pareigą supažindinti turi ne bankas, o „Smart-ID" programėlės atstovai.

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

Vertinant šiuos banko teiginius, atkreiptinas dėmesys, kad ginčo šalių sutartinių santykių neatskiriama dalimi esančiose banko mokėjimo paslaugų teikimo sąlygose ar kituose šalių sutartinius santykius reguliuojančiuose dokumentuose detaliai nėra paaiškinama, nurodoma „Smart-ID", kaip tapatybės patvirtinimo priemonės, PIN kodų suvedimo reikšmė mokėjimo operacijų vykdymo procese ir jų panaudojimo galimos pasekmės klientui, t. y. kokius veiksmus, naudodamasis „Smart-ID" programėle, banko klientas gali atlikti ir kokie veiksmai bei kokiais atvejais, naudojantis šia tapatybės patvirtinimo priemone ir suvedant jos PIN kodus, sukelia atitinkamas teisines pasekmes. Nors „Smart-ID" ir nėra banko sukurta tapatybės patvirtinimo priemonė, vis dėlto būtent bankas suteikia galimybę naudojantis ja savo klientams (šiuo atveju – pareiškėjai) nuotoliniu būdu patvirtinti savo tapatybę ir išreikšti savo valią atlikti tam tikrus veiksmus, sukeliančius jiems teisines pasekmes, t. y. naudotis banko teikiamomis paslaugomis – pateikti mokėjimo nurodymą, pasitikrinti sąskaitą ir pan. Tad banko siūlomos ir (ar) leidžiamos naudoti tapatybės patvirtinimo priemonės ne tik turi būti saugios klientams, kurie su banku susiklosčiusiuose sutartiniuose santykiuose naudoja atitinkamą tapatybės patvirtinimo priemonę, bet ir turi būti aiškios: aiškiai pateiktos jų naudojimo sąlygos ir veiksmų, atliekamų su „Smart-ID", teisinės pasekmės, pavyzdžiui, aiški PIN kodų suvedimo teisinė reikšmė. Taigi, bankas nepateikė įrodymų, kad pareiškėją buvo supažindinęs su „Smart-ID" PIN kodų naudojimo reikšme ir galimomis pasekmėmis.

Banko teigimu, pareiškėja jau nuo 2016 m. naudojosi „Smart-ID" programėle ir ja naudodamasi patvirtino ne vieną mokėjimo operaciją. Taigi, nepaisant to, kad bankas nepateikė įrodymų, kad pareiškėjai buvo suteikęs informaciją apie „Smart-ID" PIN kodų naudojimo reikšmę, atsižvelgiant į faktą, kad pareiškėja ilgą laiką naudojosi „Smart-ID" programėle, galima teigti, kad pareiškėjai vis dėlto turėjo būti žinoma „Smart-ID" PIN kodų naudojimo paskirtis, t. y. pareiškėjai buvo žinoma, kad „Smart-ID" PIN2 kodu yra tvirtinamas mokėjimo operacijų vykdymas ir kad bankas prieš mokėjimo operacijos vykdymo patvirtinimą rodo su mokėjimo operacija susijusią informaciją.

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 neautorizuotos mokėjimo operacijos iš savo sąskaitos įvykdymo. Pareiškėja turėjo galimybę tiek pastebėti, kad interneto naršyklėje jai pateikta banko interneto banko svetainės nuoroda yra besiskirianti nuo tikrosios banko interneto svetainės nuorodos, tiek ir suprasti, kad jos prašoma atlikti veiksmus, kurių nėra įprastai prašoma atlikti, o priešingai – yra prašoma atlikti veiksmus, kurie įprastai yra atliekami norint įvykdyti mokėjimo operacijas iš banko sąskaitos. Pareiškėja turėjo kritiškai įvertinti faktą, kad net 5 kartus vedant „Smart-ID" PIN1 kodą jai nepavyko patekti į savo banko sąskaitą, ir kritiškai įvertinti banko prieš vedant „Smart-ID" PIN2 kodą su mokėjimo pavedimu pareiškėjai rodytą informaciją. Tačiau, kaip ir minėta, pareiškėja, nors ir įtardama, kad prieš ją gali būti vykdoma sukčiavimo ataka, ir matydama su mokėjimo pavedimu susijusią informaciją, vis tiek suvedė „Smart-ID" PIN2 kodą ir taip patvirtino mokėjimo operacijos iš savo sąskaitos vykdymą.

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 operaciją.

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 operacijos 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 įvykdyta neautorizuota mokėjimo operacija iš pareiškėjos sąskaitos ir pareiškėja patyrė nuostolių.

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.

Įvertinus pirmiau išdėstytą informaciją, konstatuotina, kad yra pagrindas pareiškėjai taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, todėl pareiškėjos reikalavimas bankui grąžinti neautorizuotos mokėjimo operacijos sumą – 17 950 Eur, yra nepagrįstas ir atmestinas.

2. Dėl banko civilinės atsakomybės už mokėjimo operacijos įvykdymą taikymo sąlygų

Pareiškėjos atstovės teigimu, mokėjimo operacija buvo įvykdyta dėl banko kaltės, nes bankas įvykdydamas mokėjimo operaciją pažeidė PPTFPĮ 9 straipsnio 1 straipsnio 2 punktą, nes nesiėmė jokių priemonių įsitinkinti piniginės operacijos tikrumu ir legalumu ir netikrino gavėjo asmens tapatybės. Pareiškėjos atstovė kelia banko civilinės atsakomybės už pareiškėjos patirtus nuostolius dėl mokėjimo operacijos įvykdymo klausimą, iš esmės motyvuodama tuo, kad bankas pažeidė PPTFPĮ reikalavimus.

Civilinio kodekso 6.245 straipsnio 1 dalyje apibrėžiama, kad civilinė atsakomybė – tai turtinė prievolė, kurios viena šalis turi teisę reikalauti atlyginti nuostolius (žalą) ar sumokėti netesybas, o kita šalis privalo atlyginti padarytus nuostolius (žalą) ar sumokėti netesybas. Civilinė atsakomybė atsiranda esant asmens, įpareigoto atlikti atitinkamus veiksmus ar nuo jų susilaikyti, neteisėtiems veiksmams ar neveikimui, kaltei dėl šių neteisėtų veiksmų padarymo ar neveikimo, žalai ir priežastiniam ryšiui tarp veiksmų ar neveikimo ir atsiradusios žalos (Civilinio kodekso 6.246–6.249 straipsniai).

Kasacinis teismas savo praktikoje ne kartą yra pažymėjęs, kad civilinė atsakomybė kyla tik tuomet, kai nustatomos visos civilinės atsakomybės sąlygos: neteisėti veiksmai, žala, priežastinis ryšys ir kaltė, išskyrus atvejus, kai įstatyme nustatyta atsakomybė be kaltės[2]. Kai neįrodyta bent viena iš būtinųjų sąlygų, civilinė atsakomybė negali būti taikoma[3].

Pareiškėjos atstovė teigia, kad bankas įvykdydamas mokėjimo operaciją atliko neteisėtus veiksmus – pažeidė PPTFPĮ reikalavimus, todėl pareiškėjai turi būti atlyginti jos dėl mokėjimo operacijos įvykdymo patirti nuostoliai.

Vertinant pareiškėjos atstovės teiginius, kad bankas įvykdydamas mokėjimo operaciją pažeidė PPTFPĮ reikalavimus, svarbu pažymėti, kad pareiškėjos atstovė tik deklaratyviai teigė, kad bankas atliko neteisėtus veiksmus, tačiau ginčo byloje nebuvo pateikta objektyvių įrodymų, kurie pagrįstų pareiškėjos atstovės teiginį, kad bankas įvykdydamas mokėjimo operaciją pažeidė PPTFPĮ. Vadovaujantis PPTFPĮ, finansų įstaigos yra įpareigotos tinkamai pažinti savo klientus, nustatyti ir patikrinti kliento ir naudos gavėjo asmens tapatybę, gauti informaciją apie dalykinių santykių tikslą ir numatomą pobūdį, nuolat peržiūrėti ir atnaujinti kliento ir naudos gavėjo tapatybės nustatymo metu pateiktus dokumentus, duomenis ar informaciją (siekiant užtikrinti, kad minėta informacija yra tinkama ir aktuali) bei vykdyti nuolatinę kliento dalykinių santykių stebėseną, siekiant užtikrinti, kad kliento vykdomos operacijos ir sandoriai atitinka finansų įstaigos turimą informaciją apie klientą, jo verslą, rizikos pobūdį, lėšų šaltinius. Atkreiptinas dėmesys, kad nurodytos finansų įstaigų pareigos neapima pareigos pažinti ir (ar) nustatyti tapatybę asmenų, kuriems finansų įstaigos klientas siunčia lėšas, jei šie asmenys nėra pačios finansų įstaigos klientai. Finansų įstaigos, vykdydamos dalykinių santykių ir operacijų stebėseną, remiasi kliento mokėjimo nurodyme pateikiama informacija apie lėšų gavėjus. Nors finansų įstaigų pareigos apima papildomas mokėjimo nurodyme pateiktos informacijos patikras (pavyzdžiui, dėl lėšų gavėjo atitikties taikomoms tarptautinėms finansinėms sankcijoms), PPTFPĮ ar kituose teisės aktuose nėra nustatytos finansų įstaigų pareigos atlikti išsamią kiekvieno lėšų gavėjo patikrą, lygiavertę kliento atžvilgiu taikomiems reikalavimams.

Bankas Lietuvos bankui pateiktame atsiliepime taip pat paaiškino, kad teisės aktai banko neįpareigoja tikrinti kiekvienos klientų atliekamos mokėjimo operacijos, tikrinti duomenis apie kiekvieną mokėjimo nurodyme nurodytą mokėjimo operacijos sumos gavėją, analizuoti lėšų gavėjo vykdomos veiklos specifikos ar kitaip kvestionuoti mokėtojo, kuris pateikė mokėjimo nurodymą pervesti tokiam gavėjui lėšas, veiksmus.

Kaip minėta, Lietuvos bankas ginčo nagrinėjimo proceso metu neatlieka Lietuvos Respublikos Lietuvos banko įstatymo 42[1] straipsnyje reglamentuotų patikrinimų, skirtų

[2] Lietuvos Aukščiausiojo Teismo 2019 m. birželio 6 d. nutartis civilinėje byloje Nr. 3K-3-148-248/2019, 77 punktas.
[3] pvz., Lietuvos Aukščiausiojo Teismo 2010 m. balandžio 27 d. nutartis civilinėje byloje Nr. 3K-3-189/2010; 2019 m. birželio 13 d. nutartis civilinėje byloje Nr. 3K-3-1089-701/2019, 33 punktas.

faktinėms aplinkybėms, susijusioms su Lietuvos banko priežiūrimo finansų rinkos dalyvio galimai padarytu Lietuvos banko kompetencijai priskirtų teisės aktų reikalavimų pažeidimu, nustatyti ir įvertinti. Pareiškėjos atstovės teiginių apie tai, kad bankas įvykdydamas mokėjimo operaciją pažeidė PPTFPĮ, pagrįstumą būtų galima įvertinti tik atlikus Lietuvos banko įstatymo 42[1] straipsnyje reglamentuotą patikrinimą.

Svarbu tai, kad, vadovaujantis civilinio proceso rungtyniškumo principu, ginčo šalys turi įrodyti aplinkybes, kuriomis grindžia savo reikalavimus bei atsikirtimus, išskyrus atvejus, kai yra remiamasi aplinkybėmis, kurių nereikia įrodinėti (Civilinio proceso kodekso 12, 178 straipsniai).

Kaip jau buvo minėta, neteisėti veiksmai yra būtina civilinės atsakomybės sąlyga, t. y., nenustačius neteisėtų veiksmų fakto, nėra pagrindo civilinei atsakomybei kilti ir pagrindo patirtai žalai atlyginti. Nagrinėjamu atveju pareiškėjos atstovei nepateikus įrodymų, kad bankas įvykdydamas mokėjimo operaciją atliko neteisėtus veiksmus, kita civilinės atsakomybės sąlyga – priežastinis ryšys tarp žalos ir neteisėtų veiksmų – nenustatinėtina. Darytina išvada, kad, neįrodžius neteisėtų veiksmų fakto, bankui nekyla civilinė atsakomybė ir bankas neturi pagrindo atlyginti pareiškėjos prašomos atlyginti sumos – 17 950 Eur.

Į esminius šalių išdėstytus argumentus atsakyta, o kiti šalių nurodyti argumentai neturi esminės reikšmės sprendimo teisėtumui ir pagrįstumui, todėl dėl jų Lietuvos bankas plačiau nepasisako. Lietuvos banko pareiga priimti motyvuotą sprendimą neturėtų būti suprantama kaip reikalavimas detaliai atsakyti į kiekvieną šalių argumentą[4].

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

[4] Lietuvos Aukščiausiojo Teismo 2010 m. spalio 5 d. nutartis, priimta civilinėje byloje Nr. 3K-3-382/2010; 2010 m. gruodžio 20 d. nutartis civilinėje byloje Nr. 3K-3-536/2010 ir kt.