LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

SPRENDIMAS DĖL X. X. IR BANKO „SWEDBANK“, AB, GINČO NAGRINĖJIMO

2023-08-24 Nr. 429-451
Vilnius

Lietuvos bankas gavo X. X. (toliau – pareiškėja) kreipimąsi, kuriuo prašoma išnagrinėti tarp pareiškėjos ir banko „Swedbank“, AB, (toliau – bankas) kilusį ginčą.

N u s t a t y t a:

2023 m. balandžio 22 d. 23 val. 49 min. iš pareiškėjos atsiskaitomosios sąskaitos buvo atlikta 5 000 Eur mokėjimo operacija gavėjui Y. Y. (toliau – Operacija).

2023 m. balandžio 23 d. 00 val. 12 min. pareiškėja kreipėsi telefonu į banką ir pranešė, kad iš Valstybinės mokesčių inspekcijos (toliau – VMI) gavo SMS pranešimą, kuriuo buvo informuota apie skolą ir kuriame buvo pateikta aktyvi nuoroda, ją paspaudusi pareiškėja galėjo neva sumokėti skolą. Pareiškėja teigia paspaudusi aktyvią nuorodą ir atsidariusiame interneto puslapyje suvedusi prisijungimo prie banko interneto banko aplinkos duomenis. Pareiškėja taip pat nurodė, kad suvedė „Smart-ID“ PIN1 ir PIN2 kodus. Suvedusi kodus, pareiškėja pastebėjo jos sąskaitoje įvykdytą jos neautorizuotą Operaciją.

Pokalbio metu pareiškėjos mokėjimo kortelė ir teikiama interneto banko paslauga buvo užblokuotos. Taip pat pareiškėjai buvo nurodyta, kad dėl tolimesnių veiksmų (mokėjimo priemonių keitimo, prašymo dėl Operacijos lėšų grąžinimo ir pan.) pareiškėja turėtų artimiausią darbo dieną atvykti į banko padalinį.

2023 m. balandžio 24 d. pareiškėja pateikė prašymą atšaukti Operaciją, o 2023 m. balandžio 28 d. banko interneto banko aplinkoje papildomai užpildė Kliento pranešimo apie neautorizuotas operacijas sąskaitoje formą.

Atsižvelgdamas į pareiškėjos pateiktus duomenis, bankas 2023 m. balandžio 24 d. kreipėsi į lėšų gavėjo mokėjimo paslaugų teikėją dėl Operacijos atšaukimo. Papildomi priminimai apie negautą atsakymą lėšų gavėjo mokėjimo paslaugų teikėjui buvo išsiųsti dar du kartus, t. y. 2023 m. gegužės 16 d. ir 2023 m. gegužės 18 d., tačiau jokio atsakymo bankas negavo. Apie visus banko atliktus veiksmus buvo informuota ir pareiškėja.

2023 m. gegužės 8 d. banko prašymu pareiškėja patikslino Operacijos aplinkybes. Pareiškėja nurodė, kad paspaudė SMS žinutėje pateiktą aktyvią nuorodą ir suvedė visus prašomus slaptažodžius, tačiau nebuvo nukreipta prisijungti prie banko interneto puslapio, o iš karto buvo atlikta Operacija.

2023 m. gegužės 10 d., remdamasis visa surinkta informacija, bankas priėmė sprendimą atsisakyti pareiškėjai atlyginti jos patirtus nuostolius, nes nustatė, kad pati pareiškėja perdavė personalizuotus saugumo duomenis tretiesiems asmenims ir davė sutikimą atlikti Operaciją. Dėl šios priežasties bankas nurodė, kad būtent pareiškėja yra atsakinga už jos patirtus nuostolius. Taip pat bankas informavo apie tai, kad iš lėšų gavėjo mokėjimo paslaugų teikėjo atsakymo gauti nepavyko.

2023 m. gegužės 10 d. ir 2023 m. gegužės 21 d. pareiškėja kreipėsi į banką ir prašė pakartotinai apsvarstyti priimtą sprendimą, tačiau atitinkamai 2023 m. gegužės 19 d. ir 2023 m. birželio 1 d. bankas pareiškėjai pateikė atsakymus, kuriuose nurodė, kad priimtas sprendimas yra pagrįstas ir keičiamas nebus. Pareiškėja su tuo nesutiko, todėl tarp šalių kilo ginčas.

Kreipimesi į Lietuvos banką pareiškėja prašo įpareigoti banką grąžinti Operacijos metu iš pareiškėjos atsiskaitomosios sąskaitos nurašytas lėšas, t. y. 5 000 Eur. Pareiškėja nurodo, kad po sukčiavimo atakos greitai susisiekė su banku ir prašė sustabdyti Operaciją arba atlikti kitus

veiksmus, galinčius užkirsti kelią lėšų nuskaitymui, tačiau bankas nesiėmė jokių veiksmų, kurių pagrindu būtų galima atšaukti Operaciją.

Atsiliepime į pareiškėjos kreipimąsi bankas nurodo nesutinkąs su pareiškėjos reikalavimu ir prašo jį atmesti. Banko teigimu, pareiškėjai buvo sudarytos visos sąlygos susipažinti su Operacijos detalėmis ir atšaukti ją užuot patvirtinus. Taigi, banko teigimu, pareiškėjos veiksmai vienareikšmiškai laikytini kaip labai neatsargūs. Bankas nurodo, kad, net ir pareiškėjai paspaudus mygtuką „Patvirtinti" ir atsivėrus kitam „Smart-ID" ekrano langui, kuriame buvo būtina suvesti „Smart-ID" paskyros kodus, pareiškėja galėjo atšaukti Operaciją arba nesuvesti „Smart-ID" PIN2 kodo. Banko teigimu, Operacija buvo įvykdyta tik tuomet, kai „Smart-ID" PIN2 kodas buvo suvestas, todėl pareiškėjos kaltė pasireiškė būtent dideliu neatsargumu.

Banko teigimu, pareiškėja taip pat turėjo galimybę atkreipti dėmesį į netikro tinklalapio, kuris atsidarė pareiškėjai paspaudus aktyvią nuorodą, adresą. Bankas pirmiausia rekomenduoja klientams įvertinti, ar paspaudus SMS pranešimuose, el. paštu ar kitais kanalais gautas nuorodas atsidaro tikros, o ne suklastotos pardavėjo ar paslaugų teikėjo interneto svetainės, kurių vardu tokios nuorodos siunčiamos. Tai, banko teigimu, viena iš pagrindinių banko nurodytų saugaus elgesio internete vykdant finansines operacijas taisyklių, kurias bankas yra paskelbęs savo interneto svetainėje.

Banko teigimu, būtinybę saugotis netikrų pranešimų su aktyviomis nuorodomis tiek bankai, tiek policija, tiek Lietuvos bankas aktyviai ir sistemingai komunikuoja viešoje erdvėje. Taip pat ir VMI per visas žiniasklaidos priemones aktyviai kas dieną platino pranešimą su įspėjimu saugotis būtent tokių sukčiavimo atakų, nuo kokios nukentėjo ir pareiškėja.

Banko teigimu, pareiškėja dėmesio taip pat neskyrė tam, kad tinkamai susipažintų su veiksmu, kuriam patvirtinti jos prašoma duoti sutikimą naudojantis turima tapatybės patvirtinimo priemone, ir neatkreipė dėmesio į informaciją, kuri jai buvo rodoma prieš „Smart-ID" programėlės ekrane suvedant PIN1 kodą („*Prisijunkite prie Swedbank interneto banko*") ir PIN2 kodą („*Pervedimas 5000 EUR – patvirtinkite ir lėšos bus nurašytos nuo Jūsų sąskaitos. Jūsų nurodytas lėšų gavėjas: Y. Y.*"). Banko teigimu, pareiškėja savo aktyviais veiksmais leido pridėti nežinomą įrenginį, kuris buvo pavadintas „Rose's Iphone (iPhone 7)", kad būtų prisijungta prie banko interneto banko programėlės. Toks įrenginio pavadinimas galėjo ir turėjo sulaikyti pareiškėją nuo tolimesnių veiksmų ir paskatinti nedelsiant kreiptis į banką dėl turimų mokėjimo priemonių blokavimo.

Dėl šių priežasčių, remdamasis atsiliepime išdėstytais argumentais, bankas nurodo, kad pareiškėjos elgesys buvo labai neatsargus, visi nuostoliai pagal teisės aktų nuostatas turėtų tekti pačiai pareiškėjai, todėl prašo 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 Operacijos metu iš pareiškėjos atsiskaitomosios sąskaitos trečiųjų asmenų pasisavintas lėšas. Pareiškėja neigia autorizavusi Operaciją, taip pat mano, kad bankas netinkamai įvykdė jos prašymą atšaukti Operaciją, todėl privalo grąžinti Operacijos metu jos prarastas lėšas. Bankas teigia, kad tretieji asmenys įgijo sąlygas inicijuoti Operaciją tik dėl to, kad pareiškėja dėl didelio neatsargumo atskleidė savo personalizuotus saugumo duomenis tretiesiems asmenims. Remdamasis vidinės sistemos duomenimis, bankas pažymi, kad Operacija buvo patvirtinta pareiškėjos naudojama tapatybės patvirtinimo priemone („Smart-ID" paskyra), bankas mano neturintis pareigos grąžinti ir (ar) kompensuoti pareiškėjai Operacijos metu prarastos sumos.

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

Mokėjimų įstatymo 29 straipsnio 1 dalyje nustatyta, kad mokėjimo operacija laikoma

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

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

Siekiant išspręsti tarp pareiškėjos ir banko kilusį ginčą bei pasisakyti dėl pareiškėjos keliamo reikalavimo bankui pagrįstumo, Lietuvos banko vertinimu, būtina nustatyti, ar: 1) atsisakydamas grąžinti pareiškėjai Operacijos metu pervestas lėšas, bankas pagrįstai rėmėsi Mokėjimų įstatymo 39 straipsnio 3 dalimi; 2) bankas pagrįstai nesustabdė ir (ar) neatšaukė Operacijos vykdymo.

1. Dėl Mokėjimų įstatymo 39 straipsnio 3 dalies taikymo

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.

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

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

Lietuvos Aukščiausiasis Teismas yra išaiškinęs, kad didelis neatsargumas pasireiškia neprotingu arba išskirtiniu rūpestingumo nebuvimu, kai asmuo nėra tiek rūpestingas, kiek akivaizdžiai būtina esamomis aplinkybėmis[1].

Dėl mokėtojo neatsargumo laipsnio vertinimo, pagrindinių jo kriterijų ir glaudaus ryšio su ginčo byloje nustatytų individualių specifinių aplinkybių visuma Lietuvos bankas yra ne kartą plačiau pasisakęs savo ginčų nagrinėjimo praktikoje[2], todėl šiame sprendime bus pasisakoma tik šiai konkrečiai ginčo bylai aktualiais aspektais.

Neautorizuotos mokėjimo operacijos įvykdymo atveju didelis neatsargumas yra sietinas su vienos ar kelių Mokėjimų įstatymo 34 straipsnyje mokėtojui nustatytų pareigų, susijusių su mokėjimo priemone ir personalizuotais saugumo duomenimis, nevykdymu.

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

Banko mokėjimo paslaugų teikimo sąlygų (toliau – Sąlygos) 7.1 papunktyje, reglamentuojančiame su mokėjimo priemone susijusias banko kliento pareigas, nustatyta, kad: „7.1.1. Klientas, turintis teisę naudotis Mokėjimo priemone, privalo: 7.1.1.1. naudotis Mokėjimo priemone pagal Mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, nurodytas atitinkamoje Sutartyje ir / ar Paslaugos sąlygose; 7.1.1.2. sužinojęs apie Mokėjimo priemonės vagystę ar praradimą kitu būdu, įtarus ar sužinojus apie Mokėjimo priemonės

[1] Lietuvos Aukščiausiojo Teismo 2017 m. balandžio 13 d. nutartis civilinėje byloje Nr. e3K-3-180-378/2017.
[2] Pavyzdžiui, ginčo bylos Nr. 2022-00586 ir 2022-02496.

neteisėtą įgijimą arba neautorizuotą jos naudojimą, taip pat apie faktus ar įtarimus, kad Mokėjimo priemonės personalizuotus saugumo duomenis (įskaitant Tapatybės patvirtinimo priemones) sužinojo arba jais gali pasinaudoti Tretieji asmenys, nedelsdamas apie tai pranešti Bankui ar kitam jo nurodytam subjektui, vadovaujantis Mokėjimo priemonės išdavimą ir naudojimą reglamentuojančiomis sąlygomis, nurodytomis Sutartyje ir / ar Paslaugos sąlygose. 7.1.2. Klientas, gavęs Mokėjimo priemonę, privalo iš karto imtis visų veiksmų (įskaitant nurodytus Paslaugos sąlygose ir atitinkamoje Sutartyje), kad būtų apsaugoti gautos Mokėjimo priemonės personalizuoti saugumo duomenys (įskaitant Tapatybės patvirtinimo priemones)."

Taigi, pirmiau aptartos mokėjimo kortelės sutarties (ją sudarančių dokumentų) nuostatos aiškiai nustato, kad už mokėjimo ir tapatybės patvirtinimo priemonių personalizuotų saugumo duomenų konfidencialumą yra atsakingas mokėtojas, šiuo atveju – pareiškėja, ji privalo užtikrinti, kad minėti duomenys netaptų žinomi tretiesiems asmenims. Atsižvelgiant į tai, manytina, kad pareiškėjos elgesys būtų laikomas kaip atitinkantis mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, jei būtų nustatyta, kad pareiškėja ėmėsi adekvačių veiksmų (arba priešingai – nustačius, kad nuo tam tikrų veiksmų susilaikė) tam, kad jai banko išduotų mokėjimo priemonių personalizuotų saugumo duomenų, įgalinančių inicijuoti ir tvirtinti mokėjimus, konfidencialumas būtų tinkamai užtikrintas ir jie būtų naudojami šalių sutartinius santykius reglamentuojančių dokumentų nustatyta tvarka bei sąlygomis.

Vis dėlto, įvertinus ginčo byloje esančius duomenis ir ginčo nagrinėjimo metu nustatytas aplinkybes, išvados, kad pareiškėjos elgesys atitiko banko nustatytas naudojimosi mokėjimo priemonėmis sąlygas ir buvo adekvatus, pakankamas tam, kad pareiškėjai nustatytos pareigos, susijusios su mokėjimo priemonių personalizuotų saugumo duomenų konfidencialumo užtikrinimu, būtų tinkamai įvykdytos, daryti negalima.

Nors pareiškėjai atsiųstas SMS pranešimas galėjo sukurti pirminį įspūdį, kad šis pranešimas išsiųstas potencialiai VMI, tačiau tai, kad pareiškėja iki personalizuotų duomenų atskleidimo (pateikimo suklastotoje interneto svetainėje) nesudvejojo pranešime nurodytos informacijos ir jai nepažįstamo siuntėjo patikimumu, leidžia teigti, kad pareiškėjos elgesys Operacijos inicijavimo metu nebuvo itin apdairus ir atsargus.

Pirma, pažymėtina, kad pareiškėja, paspaudusi SMS pranešime pateiktą aktyvią nuorodą, buvo nukreipta į suklastotą VMI tinklalapį, kuriame, pasirinkusi, jog yra banko klientė, turėjo suvesti visus prisijungimui prie pareiškėjos banko sąskaitos reikalingus duomenis, t. y. naudotojo ID ir asmens kodą. Taip tretieji asmenys įgijo galimybę inicijuoti prisijungimą prie pareiškėjos banko interneto banko aplinkos.

Atlikus šiuos veiksmus, pareiškėjos „Smart-ID" programėlės ekrane pasirodė pranešimas, kad ji jungiasi prie banko interneto banko aplinkos, todėl pareiškėja suvedė „Smart-ID" paskyros PIN1 kodą, kuris leido tretiesiems asmenims prisijungti prie pareiškėjos banko interneto banko paskyros. Kad tretieji asmenys galėtų naudotis būtent jų mobiliajame įrenginyje įdiegta banko išmaniąja programėle, pareiškėja turėjo patvirtinti pridėtą papildomą mobilųjį įrenginį, iš kurio pirmą kartą jungėsi tretieji asmenys. Pareiškėjai į „Smart-ID" paskyrą buvo atsiųstas pranešimas, kuriame prašoma patvirtinti naujai pridedamą įrenginį[3]. Iš banko pateiktų objektyvių duomenų matyti, kad sutikimą jos vardu naudotis banko programėle kitame įrenginyje pareiškėja davė naudodamasi savo mobiliuoju įrenginiu ir panaudodama tik jai vienai žinomus „Smart-ID" paskyros PIN kodus. Nors iš banko pateiktų duomenų matyti, kad pareiškėja naudojosi *iOs iPhone XR* mobiliuoju įrenginiu, pareiškėjai nekilo įtarimų, kad ji suteikia galimybę naudojantis banko mobiliąja programėle jungtis asmenims, kurie naudoja visai kitą įrenginį (*Rose's iPhone (iPhone 7*)). Taigi, pareiškėja tiek suvesdama PIN1 kodą, tiek patvirtindama įrenginį leido tretiesiems asmenims prisijungti prie pareiškėjos banko interneto banko paskyros ir inicijuoti Operaciją.

Antra, pareiškėja neskyrė pakankamai dėmesio ir tam, kad tinkamai susipažintų su veiksmu, kurį jos prašoma patvirtinti, t. y. kad buvo prašoma patvirtinti Operaciją. Pareiškėjai pateiktame „Smart-ID" programėlės pranešime, prašančiame suvesti PIN2 kodą ir patvirtinti Operaciją, buvo aiškiai ir nedviprasmiškai nurodyta, kokia suma tvirtinama, kad lėšos bus nurašytos iš pareiškėjos sąskaitos ir kas yra Operacijos lėšų gavėjas[4].

Taigi, vertinant pareiškėjos elgesį būtent nagrinėjamo ginčo aplinkybių ir prieš pareiškėją nukreiptos specifinės sukčiavimo atakos kontekste, esminėmis aplinkybėmis, vertinant pareiškėjos neatsargumo laipsnį, Lietuvos banko vertinimu, laikytina tai, kad

[3] Pranešimo tekstas: „Patvirtinkite šį įrenginį Rose's IPhone (iPhone 7) programėlės naudojimui."

[4] Pareiškėjai rodomos žinutės tekstas: „Pervedimas 5000 Eur – patvirtinkite ir lėšos bus nurašytos nuo Jūsų sąskaitos. Jūsų nurodytas lėšų gavėjas: Reclavs Janis.").

pareiškėjai nesukėlė jokių įtarimų tai, kad jos yra prašoma patvirtinti, kad per banko mobiliąją programėlę prie pareiškėjos sąskaitos jungiamasi su visiškai kitu, nei pareiškėja naudoja, įrenginiu. Be to, nors pareiškėjai buvo pateikta aiški ir nedviprasmiška informacija, kokia suma, kokiu būdu ir kam yra atliekama Operacija, ji nepaisė jai atsiųstame pranešime nurodytos informacijos ir vis tiek patvirtino šią Operaciją.

Kaip minėta, pagal banko mokėjimo paslaugų teikimo sąlygas, mokėjimo kortelės personalizuotų saugumo duomenų pateikimas minėtose sąlygose numatytais atvejais laikomas kliento (šiuo atveju – pareiškėjos) sutikimu įvykdyti mokėjimo operaciją, lėšas nurašant iš kliento (šiuo atveju – pareiškėjos) sąskaitos. Atitinkamai ginčo byloje nėra jokių duomenų, kad pareiškėja būtų kvestionavusi SMS pranešime nurodytą tekstą ir pateiktos nuorodos tikrumą, o jei tokių abejonių turėjo, nėra jokių duomenų, kad šias abejones būtų bandžiusi išsklaidyti, patikrinti gautą informaciją. Pareiškėjai nesukėlė įtarimų jai atsiųstas SMS pranešimo, kuris yra parašytas be lietuviškų raidžių, turinys, o pranešime pateikta nuoroda taip pat skiriasi nuo VMI naudojamos interneto banko nuorodos[5].

Vadovaujantis banko viešai skelbiamomis saugaus naudojimosi elektroninėmis paslaugomis rekomendacijomis banko klientai raginami nespausti jokių el. paštu, pokalbių programėlėse ar SMS žinutėse gautų nuorodų, nevykdyti prašymų suvesti arba padiktuoti prisijungimo prie interneto banko ar kortelės duomenis, atidžiai įvertinti savo telefono ekrane matomą prašymą įvesti turimos prisijungimo priemonės slaptažodį, jei nėra su kuo sulyginti kontrolinio kodo arba jis nesutampa, arba ignoruoti tokį pranešimą, jei nesiekiama prisijungti prie interneto banko ar inicijuoti mokėjimo operacijų, kilus nors mažiausiai abejonei, neskubėti ir nedelsiant nutraukti veiksmus[6]. Tokia pati informacija yra skelbiama ir „Smart-ID" naudotojo atmintinėje, kuri yra neatskiriama pareiškėjos ir banko sudarytos sutarties dalis[7]. Taip pat bankas pateikė duomenis, kad el. bankininkystės sistemoje 2020 m. balandžio 2 d., 2021 m. gruodžio 9 d. bei 2022 m. rugsėjo 29 d. pareiškėja asmeniškai buvo įspėta, kad būtų budri, nes sukčiai aktyviai išvilioja bankų klientų duomenis.

Taigi, iš šių duomenų matyti, kad bankas, būdamas savo srities profesionalas, prevenciškai dėjo pastangas tam, kad pareiškėja būtų supažindinta su sukčiavimo elektroninėje erdvėje rizikomis bei tapatybės patvirtinimo priemonės saugaus naudojimo, jos personalizuotų saugumo žymenų suvedimo ir atskleidimo reikšme bei teisinėmis pasekmėmis.

Iš banko pateiktų duomenų matyti, kad ir VMI nuo 2023 m. balandžio 11 d. aktyviai platino pranešimus, kuriuose skatino visus asmenis saugotis būtent tokio paties pobūdžio sukčiavimo atakų, nuo kokios nukentėjo ir pareiškėja.[8] Taigi, pareiškėja turėjo galimybę susipažinti ir su tokių sukčiavimo atakų pobūdžiu dar iki konkrečiai prieš pareiškėją nukreiptos sukčiavimo atakos.

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

Kaip matyti iš nustatytų aplinkybių, Operaciją tretieji asmenys be pareiškėjos žinios galėjo atlikti tik dėl to, kad pareiškėja, būdama labai neatsargi, netinkamai įvykdė Mokėjimų įstatyme (34 straipsnis) ir su banku sudarytoje mokėjimo kortelės sutartyje įtvirtintus mokėjimo kortelės saugaus naudojimo reikalavimus. Remiantis nustatytais duomenimis, pareiškėja, gavusi trečiųjų asmenų siųstą pranešimą, nedvejodama (kaip pripažįsta) paspaudė jame pateiktą nuorodą ir suklastotame interneto puslapyje nurodė savo personalizuotus saugumo duomenis, neįsitikinusi siųsto pranešimo ir jame pateiktos nuorodos tikrumu. Taip pat pareiškėja, neįvertinusi jai „Smart-ID" programėlėje siųstų pranešimų turinio, patvirtino trečiųjų asmenų galimybę naudotis pareiškėjos banko interneto banko paskyra per būtent jų mobiliajame įrenginyje įdiegtą banko išmaniąją programėlę. Galiausiai pareiškėja neįvertino į pareiškėjos „Smart-ID" paskyrą siųsto pranešimo, kuriame nurodoma tvirtinamos Operacijos informacija, turinio ir savo aktyviais veiksmais galiausiai patvirtino Operaciją.

Nurodytos aplinkybės leidžia teigti, kad pareiškėja būtent dėl savo didelio neatsargumo neišsaugojo personalizuotų saugumo duomenų konfidencialumo – nesiėmė tų saugumo priemonių, kurių privalėjo imtis, kad būtų tinkamai apsaugoti jai suteiktos mokėjimo priemonės

---

[5] SMS pranešimo tekstas: „Gavote nauja pranesima su informacija apie nesumoketa bauda, prisijunkite cia vmi.lt-prisijungti-i.net."

[6] https://www.swedbank.lt/private/d2d/ebanking/secureBanking?language=LIT

[7] https://www.swedbank.lt/static/pdf/private/home/more/Smart_ID_atmintine_2019-11.pdf

[8] https://www.vmi.lt/evmi/en/-/vmi-c4-afsp-c4-97ja-gyventojus-gavus-c4-aftartin-c4-85-prane-c5-a1im-c4-85-neskub-c4-97kite-atidaryti-nuorod-c5-b3

duomenys, ir pati patvirtino Operaciją.

Konstatavus, kad pareiškėja, nesilaikydama jai, kaip mokėtojai, Mokėjimų įstatyme ir sutartyje su banku nustatytų pareigų, susijusių su išduotomis mokėjimo priemonėmis, elgėsi labai neatsargiai, kartu darytina išvada, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, nustatančią, kad tokiu atveju mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai. Dėl šios priežasties, Lietuvos banko vertinimu, bankas neturi pareigos grąžinti (kompensuoti) pareiškėjai neautorizuotos Operacijos lėšų.

2. Dėl mokėjimo nurodymo neatšaukiamumo

Pareiškėja kreipimesi, be kita ko, nurodė, kad kreipėsi į banką iš karto po atliktos Operacijos, todėl bankas privalėjo sustabdyti Operacijos vykdymą ir taip apsaugoti pareiškėjos lėšas.

Vertinant galimybę atšaukti pareiškėjos vardu pateiktą mokėjimo nurodymą įvykdyti Operaciją, papildomai pažymėtina, kad, vadovaujantis Mokėjimų įstatymo 44 straipsnio 1 dalimi, mokėjimo paslaugų vartotojas negali atšaukti mokėjimo nurodymo po to, kai jį gauna mokėtojo mokėjimo paslaugų teikėjas, išskyrus šiame straipsnyje nustatytas išimtis. Minėto Mokėjimų įstatymo straipsnio 4 dalyje taip pat, be kita ko, 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.

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 Mokėjimų įstatymo 44 straipsnio 1 dalyje nurodytam terminui).

Sąlygų 3.3.5 papunktyje yra nustatyta mokėjimo nurodymo atšaukimo tvarka. Sąlygų 3.3.5.1 papunktyje yra nustatyta, kad mokėjimo nurodymas negali būti atšauktas po to, kai jį gauna bankas, išskyrus Sąlygose numatytus atvejus.

Bankas atsiliepime paaiškino, kad Operacija buvo įvykdyta dar iki pareiškėjos pirmojo kreipimosi į banką. Banko teigimu, Operacija buvo įvykdyta kaip momentinis mokėjimas, todėl lėšos per keliolika sekundžių pasiekė lėšų gavėjo mokėjimo paslaugų teikėją, iš kurio tretieji asmenys turėjo galimybę akimirksniu pasiimti lėšas. Bankas pažymi, kad neturėjo jokių techninių galimybių sustabdyti Operacijos (momentinio mokėjimo), kol Operacijos lėšos dar nebuvo išsiųstos iš banko, ar vėliau jų atšaukti.

Nustatytais duomenimis, nei Mokėjimų įstatyme, nei šalių susitarime nurodytos sąlygos atšaukti mokėjimo nurodymą įvykdyti Operaciją nebuvo nustatytos, t. y. pareiškėja į banką su prašymu atšaukti mokėjimo nurodymą įvykdyti Operaciją ir (ar) grąžinti šio mokėjimo lėšas į pareiškėjos mokėjimo kortelės sąskaitą paskambino po to, kai Operacija jau buvo įvykdyta, taigi, ir Mokėjimų įstatyme bei šalių susitarime nustatytas terminas atšaukti mokėjimo nurodymus jau buvo praėjęs ir bankas neturėjo jokių galimybių Operaciją atšaukti.

Įvertinus visa tai, kas išdėstyta pirmiau, ir nustačius, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, darytina išvada, kad pareiškėjos bankui keliamas reikalavimas grąžinti Operacijos sumą – 5 000 Eur, yra nepagrįstas, todėl atmestinas.

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

Atmesti pareiškėjos X. X. reikalavimą.

Lietuvos banko sprendimas dėl ginčo esmės yra rekomendacinio pobūdžio ir teismui neskundžiamas. Vartotojui ir finansų rinkos dalyviui išlieka teisė dėl ginčo sprendimo kreiptis į teismą įstatymų nustatyta tvarka. Kreipimasis į teismą po Lietuvos banko sprendimo dėl ginčo esmės priėmimo nelaikomas šio sprendimo apskundimu. Ginčo šalys turi pareigą pranešti

Lietuvos bankui, jeigu viena iš ginčo šalių pareiškia ieškinį bendrosios kompetencijos teismui prašydama nagrinėti tapatų ginčą iš esmės.

Direktorius Arūnas Raišutis