LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

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

2023-03-08 Nr. 429-134
Vilnius

Lietuvos bankas gavo X.X. (toliau – pareiškėjas) kreipimąsi, kuriuo prašoma išnagrinėti tarp pareiškėjo ir AB SEB banko (toliau – bankas) kilusį ginčą.

N u s t a t y t a:

Pareiškėjas 2022 m. rugpjūčio 6 d. telefonu gavo SMS pranešimą su nuoroda. Paspaudus trečiųjų asmenų atsiųstą nuorodą, atsidarė netikras banko interneto puslapis, imituojantis banko interneto banko puslapį, jame buvo prašoma įvesti pareiškėjui asmeniškai suteiktus unikalius duomenis – interneto banko atpažinimo kodą ir asmens kodą, būtinus prisijungti prie interneto banko, o vėliau suvesti ir pareiškėjo naudojamos atpažinties priemonės „Smart-ID" paskyros PIN1 kodą. Suvedus minėtus duomenis, tretieji asmenys savo mobiliojo telefono įrenginyje pareiškėjo vardu įdiegė banko mobiliąją programėlę (toliau – programėlė) bei sukūrė naujus programėlės PIN kodus, kurių sukūrimą pareiškėjas patvirtino suvesdamas „Smart-ID" paskyros PIN2 kodą. Taip tretieji asmenys įgijo galimybę iš pareiškėjo sąskaitos banke pareiškėjo vardu inicijuoti mokėjimo operacijas ir atlikti kitus veiksmus. Tretieji asmenys pasinaudodami programėle pareiškėjo vardu 2022 m. rugpjūčio 6 d. inicijavo dvi mokėjimo operacijas, kurių bendra suma – 3 000 Eur (toliau – mokėjimo operacijos).

Bankui atsisakius grąžinti pareiškėjui jo neautorizuotų mokėjimo operacijų sumą, pareiškėjas kreipėsi į Lietuvos banką dėl vartojimo ginčo nagrinėjimo. Kreipimesi pareiškėjas teigė: „is sukciu gavus zinute su nurodymu kad mano saskaita uzblokuota,as suvedziau savo asmens koda ir atpazinimo koda,po to PIN1 ir PIN2 taip tretieji asmenys susikure programele mano vardu.As iskarto paskambinau i banka ir informavau,bet jau buvo per velu.Sukciai is mano saskaitos pervede i kita saskaita 2000eur ir 1000eur!" Pareiškėjas teigė nedavęs sutikimo vykdyti mokėjimo operacijų ir nemano, kad jos buvo įvykdytos dėl pareiškėjo didelio neatsargumo. Pareiškėjo nuomone, bankas turi prisiimti atsakomybę už iš pareiškėjo sąskaitos įvykdytas mokėjimo operacijas.

Bankas nesutinka tenkinti pareiškėjo reikalavimo, nes jis elgėsi itin neapdairiai: paspaudė neaiškią nuorodą, suvedė savo interneto banko ID, asmens kodą ir savo mobiliajame įrenginyje savo atliekamus veiksmus patvirtino suvesdamas tik jam žinomus „Smart-ID" paskyros PIN1 ir PIN2 kodus, dėl to tretieji asmenys galėjo pareiškėjo vardu susikurti programėlę ir taip inicijuoti mokėjimo operacijas bei jas patvirtinti.

Atsiliepime pažymima, kad nors pareiškėjas teigia neautorizavęs mokėjimo operacijų, tačiau banko sistemų išrašai rodo, kad mokėjimo operacijos buvo patvirtintos banko ir pareiškėjo sudarytoje sutartyje sutartu būdu – panaudojus tik pareiškėjui žinomus personalizuotus saugos duomenis: interneto banko ID, asmens kodą, „Smart-ID" paskyros PIN1 ir PIN2 kodus. Bankas pažymėjo, kad, prieš pareiškėjui vedant Smart-ID" paskyros PIN1 kodą, jam buvo rodoma informacija – *Login to SEB*, o prieš vedant „Smart-ID" paskyros PIN2 kodą pareiškėjui buvo rodoma informacija – *kuriate naujus SEB programos PIN kodus. Patvirtinkite mobiliosios programėlės sukūrimą.*

Banko nuomone, mokėjimo operacijos turi būti laikomos pareiškėjo autorizuotomis. Mokėjimo operacijoms tvirtinti bankas taiko papildomą kliento ir jo operacijų autentifikavimą, taip siekdamas suteikti galimybę klientui įsitikinti inicijuojamos operacijos teisėtumu. Klientams įvykdžius visas banko ir kliento sutartas sąlygas, kad kliento inicijuota operacija būtų tinkamai

identifikuota, bankas įsipareigoja tokias operacijas įvykdyti. Bankas nurodo, kad vykdant mokėjimo operacijas banko sistemos veikė saugiai, jokių sutrikimų užfiksuota nebuvo. Įvertinęs aplinkybių visumą ir teisinį reglamentavimą, bankas mano neturintis pareigos pareiškėjui kompensuoti nuostolių, patirtų dėl įvykdytų mokėjimo operacijų.

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 (toliau – Taisyklės) 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.

Pareiškėjo ir banko ginčas kilo dėl banko atsisakymo grąžinti ir (ar) kompensuoti pareiškėjui jo ginčijamų mokėjimo operacijų, įvykdytų dėl trečiųjų asmenų surengtos sukčiavimo atakos, sumą.

Pareiškėjas teigia, kad bankas įvykdė neautorizuotas mokėjimo operacijas, nes pareiškėjas pats jų neinicijavo ir nepatvirtino. Bankas teigia, kad tretieji asmenys įgijo sąlygas inicijuoti mokėjimo operacijas tik dėl to, kad pareiškėjas dėl didelio neatsargumo atskleidė savo mokėjimo priemonių personalizuotus saugumo duomenis tretiesiems asmenims ir mokėjimo operacijas patvirtino suvesdamas savo naudojamos „Smart-ID" paskyros PIN1 ir PIN2 kodus, todėl mokėjimo operacijų lėšų grąžinti ir (ar) kompensuoti pareiškėjui bankas neturi pareigos.

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.

Lietuvos banko vertinimu, siekiant išspręsti tarp pareiškėjo ir banko kilusį ginčą bei pasisakyti dėl pareiškėjo keliamo reikalavimo pagrįstumo, būtina nustatyti, ar: 1) mokėjimo operacijos laikytinos autorizuotomis; 2) bankas turėjo (turi) pareigą grąžinti (kompensuoti) pareiškėjui mokėjimo operacijų sumą.

1. Dėl ginčijamų 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 įstatymo 37 straipsnio 1 dalyje nustatyta, kad tuo atveju, jeigu mokėtojas neigia autorizavęs įvykdytą mokėjimo operaciją ar teigia, kad mokėjimo operacija buvo įvykdyta netinkamai, jo mokėjimo paslaugų teikėjas turi įrodyti, kad mokėjimo operacijos autentiškumas buvo patvirtintas, ji buvo tinkamai užregistruota, įrašyta į sąskaitas ir jos nepaveikė techniniai trikdžiai arba kiti mokėjimo paslaugų teikėjo teikiamos paslaugos trūkumai; kai mokėtojas neigia autorizavęs įvykdytą mokėjimo operaciją, mokėtojo mokėjimo paslaugų teikėjo arba atitinkamais atvejais mokėjimo inicijavimo paslaugos teikėjo užregistruotas mokėjimo priemonės naudojimas nebūtinai yra pakankamas įrodymas, kad mokėtojas autorizavo mokėjimo operaciją ar veikė nesąžiningai arba tyčia ar dėl didelio neatsargumo neįvykdė vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų.

Pažymėtina, kad Mokėjimų įstatyme nėra nustatytų konkrečių mokėtojo sutikimo įvykdyti mokėjimo operaciją būdų ir (arba) išsamios 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 jo mokėjimo paslaugų teikėjo sudaromoje bendrojoje mokėjimo paslaugų teikimo sutartyje (toliau – bendroji sutartis).

Ginčo šalių sutartinių santykių neatskiriama dalimi esančių banko Bendrųjų taisyklių 1 priedo 3 skyriuje nustatyta, kad sutikimą atlikti mokėjimo operaciją mokėtojas gali duoti „<…> patvirtindamas elektroniniu parašu, naudodamas mūsų suteiktas atpažinimo priemones (slaptažodžius, kodus, kitus personalizuotus saugumo duomenis) interneto banke arba SEB

mobiliojoje programėlėje, kitu su mumis sutartu ar banko nustatytu būdu".

Darydamas išvadą, kad mokėjimo operacijos buvo atliktos tinkamai, taigi, šalių sutarta tvarka buvo išreikštas pareiškėjo sutikimas, bankas remiasi banko vidinės sistemos duomenimis, kurie patvirtina, kad mokėjimo operacijoms įvykdyti buvo panaudoti pareiškėjo interneto banko prisijungimo duomenys – interneto banko naudotojo ID kodas ir pareiškėjo vardu išduotos atpažinimo priemonės „Smart-ID" PIN1 (prisijungti prie interneto banko) ir PIN2 (patvirtinti programėlės įdiegimą kitame įrenginyje ir naujų PIN kodų sukūrimą) kodai. Atsižvelgdamas į tai, kad mokėjimo operacijos buvo patvirtintos šalių sutartu būdu, taikant griežtą kliento tapatybės nustatymo procesą, bankas mano, kad nėra pagrindo laikyti mokėjimo operacijų neautorizuotomis.

Darydamas išvadą, kad mokėjimo operacijos buvo tinkamai pareiškėjo patvirtintos ir laikytinos autorizuotomis, bankas papildomai nevertino mokėjimo operacijų inicijavimo ir patvirtinimo aplinkybių: kas perdavė lėšų gavėjui ir (arba) jo mokėjimo paslaugų teikėjui duomenis, kurių pagrindu buvo inicijuotos mokėjimo operacijos, t. y. ar šiuos duomenis tiesiogiai pateikė pats pareiškėjas, ar iš pareiškėjo šiuos duomenis neteisėtai išvilioję tretieji asmenys. Lietuvos banko vertinimu, vien faktas, kad mokėjimo operacijos papildomai patvirtintos pagal griežtą tapatybės nustatymo procesą, t. y. trečiųjų asmenų įrenginyje įdiegus programėlę, kurios įdiegimas patvirtintas papildomai suvedus tik pareiškėjui žinomą jo naudojamos tapatybės patvirtinimo priemonės „Smart-ID" paskyros PIN2 kodą, savaime dar nereiškia, kad mokėjimo operacijos buvo atliktos su pareiškėjo sutikimu.

Siekdamas pagrįsti teiginį, kad mokėjimo operacijoms atlikti buvo tinkamai, t. y. šalių sutartu būdu, duotas pareiškėjo sutikimas, bankas remiasi pirmiau aptartomis banko Bendrųjų taisyklių nuostatomis. Vis dėlto minėtose banko Bendrųjų taisyklių nuostatose kalbama apie atvejus, kai *mokėtojas* duoda savo sutikimą pervesti lėšas ir tuo tikslu panaudoja jam išduotas mokėjimo ir tapatybės patvirtinimo priemones (jų duomenis). Tačiau nustatyta, kad pareiškėjas, priešingai, nei nurodyta aptariamose nuostatose, savo prisijungimo prie interneto banko duomenis panaudojo fiktyvioje – į telefoną gautoje SMS žinutėje pateiktą nuorodą paspaudus atsiradusioje, interneto svetainėje ir suvedė juos ne dėl to, kad ketino pervesti lėšas, siekdamas atsiskaityti už suteiktas paslaugas ar įsigytas prekes, o vykdydamas gautoje žinutėje pateiktus nurodymus ir siekdamas atlikti veiksmus, kad tariamai būtų atblokuota paskyra.

Lietuvos banko vertinimu, tais atvejais, kai nustatomi duomenys, kad mokėtojo (vartotojo) per neatsargumą atskleistais mokėjimo priemonių personalizuotais saugumo duomenimis neteisėtai pasinaudoja tretieji asmenys ir mokėtojo vardu juos pateikia tam, kad būtų inicijuotas mokėjimo nurodymas atlikti lėšų pervedimo operaciją, tokios mokėjimo operacijos negali būti laikomos operacijomis, kurioms įvykdyti buvo duotas mokėtojo sutikimas Mokėjimų įstatymo 29 straipsnio 1 dalies prasme. Trečiojo asmens veiksmai, kuriais pateikiamas mokėjimo nurodymas įvykdyti lėšų pervedimo operaciją mokėtojo vardu, nors formaliai ir atitinka mokėtojo ir mokėjimo paslaugų teikėjo sutartą sutikimo atlikti mokėjimo operaciją davimo formą, negali būti laikomi tinkamu mokėtojo sutikimu atlikti tokią mokėjimo operaciją, esant duomenų, kad jie neatitinka mokėtojo tikrosios valios.

Bankas atsiliepime taip pat teigia, kad sutikimo faktui konstatuoti neturi būti remiamasi vien tik pareiškėjo subjektyviu vertinimu dėl to, ar mokėjimo operacijos laikytinos autorizuotomis, tačiau turi būti vertinami konkretūs pareiškėjo atlikti veiksmai ir ar jie atitinka su banku sutarto sutikimo atlikti mokėjimo operaciją kriterijų.

Atsižvelgdamas į šiuos banko teiginius, Lietuvos bankas pažymi, kad, kaip buvo nurodyta pirmiau, vien tik aplinkybė, jog mokėtojo mokėjimo paslaugų teikėjo vidaus sistemose užregistruotas mokėtojui išduotos mokėjimo priemonės, įskaitant jos personalizuotus saugumo duomenis, naudojimas, nelaikytina pakankamu įrodymu, kad mokėjimo priemone tikrai naudojosi pats vartotojas ir (arba) kad tokia mokėjimo operacija laikytina tinkamai mokėtojo autorizuota. Nesant objektyvių įrodymų, kad, inicijuojant šalių sutartu būdu patvirtintą ir vartotojo ginčijamą mokėjimo operaciją, vartotojo mokėjimo priemone ir jos personalizuotais saugumo duomenimis be vartotojo žinios ir valios galėjo pasinaudoti tretieji asmenys, ir esant tik subjektyviems vartotojo paaiškinimams, įprastai tokia mokėjimo operacija laikytina autorizuota.

Lietuvos bankas pažymi, kad valia yra esminis kiekvieno sandorio, kaip teisinio veiksmo, kuriuo siekiama sukurti tam tikras teises ir pareigas, elementas[1]. Tai reiškia, kad, nesant

[1] „Apgaulės atveju sudarytas sandoris yra ne sandorio šalies laisvos valios išraiškos rezultatas, o kitos sandorio šalies ar trečiojo asmens nesąžiningų veiksmų rezultatas. Jeigu apgaulės nebūtų buvę, apgautoji sandorio šalis sandorio arba apskritai nebūtų sudariusi, arba būtų sudariusi jį visiškai kitokiomis sąlygomis." (Lietuvos Aukščiausiojo Teismo

mokėtojo valios inicijuoti lėšų pervedimo operacijos, toks mokėjimo nurodymas, nors formaliai ir patvirtintas šalių sutarta sutikimo atlikti mokėjimo operaciją davimo forma, negali būti laikomas tinkamai autorizuotu paties mokėtojo, turint duomenų, kad tokiam mokėjimo nurodymui pateikti pats mokėtojas savo valios neišreiškė, nesuprato, o tam tikrais atvejais ir negalėjo žinoti, kad jo vardu yra pateikiamas mokėjimo nurodymas pervesti lėšas.

Mokėtojo valia pateikti konkretų mokėjimo nurodymą mokėjimo paslaugų teikėjui yra esminė aplinkybė, vertinant, ar ginčijama mokėjimo operacija laikytina autorizuota, tačiau, kaip minėta pirmiau, tinkama mokėtojo valios išraiškos forma vertintina ne tik vertinant mokėtojo nuomonę, teiginius apie mokėjimo nurodymo pateikimo ir ginčijamos mokėjimo operacijos įvykdymo aplinkybes, tačiau analizuotinos ir mokėtojo valios išraišką atspindinčios ir pagrindžiančios mokėjimo nurodymo pateikimo ir ginčijamos mokėjimo operacijos įvykdymo aplinkybės. Tais atvejais, kai ginčijama mokėjimo operacijos autorizavimo aplinkybė, turi būti vertinama, kas ir kaip inicijavo mokėjimo operaciją ir (ar) pateikė mokėjimo paslaugų teikėjui duomenis, būtinus mokėjimo operacijai inicijuoti ir patvirtinti, taip pat turi būti analizuojamos ir visos kitos aplinkybės, pagrindžiančios arba paneigiančios vartotojo (mokėtojo) teiginį, kad valios inicijuoti ir (ar) patvirtinti ginčijamą mokėjimo operaciją vartotojas (mokėtojas) neturėjo.

Be to, sprendžiant, ar konkreti mokėjimo paslaugų vartotojo ginčijama operacija (šiuo atveju – pareiškėjo ginčijamos mokėjimo operacijos) laikytina autorizuota, svarbu įvertinti, ar faktinės ginčijamų mokėjimo operacijų inicijavimo ir tvirtinimo aplinkybės, kurias pagrindžia ginčo byloje esantys duomenys, atitinka šalių sudarytoje sutartyje aptartą mokėjimo operacijų autorizavimo tvarką.

Iš ginčo byloje esančių duomenų matyti, kad pareiškėjas iš trečiųjų asmenų gavo SMS žinutę, įterptą į tikrų banko žinučių srautą. Pareiškėjui išsiųstu pranešimu pareiškėjas informuojamas apie tariamą jo paskyros apribojimą ir raginamas spausti šalia pateiktą nuorodą *„mes užblokavome jusu saskaita del neteistu mokėjimu i kitas saskaitas. Prisijunkite cia norėdami atblokuoti – https://seb-ltsaskaita.net"*.

Įvertinus pirmiau aptartus duomenis, konstatuotina, kad, spausdamas gautoje SMS žinutėje pateiktą nuorodą ir pagal ją atsidariusiame interneto puslapyje suvesdamas prašomus pateikti duomenis, pareiškėjas siekė atlikti veiksmus tariamam paskyros apribojimui panaikinti, o ne inicijuoti mokėjimo nurodymus lėšų pervedimams iš banke esančios pareiškėjo sąskaitos.

Taigi, banko teiginio ir vertinimo, kad pats pareiškėjas išreiškė savo valią ir sutikimą atlikti mokėjimo operacijas šalių sutarta forma ir tvarka, nepatvirtina nustatytos aplinkybės. Remiantis aplinkybe, kad pareiškėjas prisijungimo prie interneto banko duomenis, vėliau panaudotus siekiant trečiųjų asmenų mobiliajame įrenginyje pareiškėjo vardu įdiegti programėlę ir inicijuoti mokėjimo operacijas, suvedė trečiųjų asmenų sukurtame fiktyviame banko interneto banko puslapyje, sukūrusiame įspūdį, kad pareiškėjo prašoma pateikti duomenis paskyros apribojimams panaikinti, galima daryti išvadą, kad mokėjimo operacijų inicijavimas ir patvirtinimas neatitiko pačio pareiškėjo valios, nors formaliai (pagal išorinius požymius) ir sutapo su pareiškėjo ir banko sutarta sutikimo atlikti mokėjimo operacijas davimo forma ir tvarka.

Lietuvos banko nuomone, vertinti mokėjimo operacijų kaip autorizuotų – atliktų esant pačio pareiškėjo sutikimui (kaip tai suprantama Mokėjimų įstatymo 29 straipsnio 1 dalies kontekste), nėra pagrindo, todėl Lietuvos bankas daro išvadą, kad mokėjimo operacijos laikytinos neautorizuotomis.

2. Dėl neautorizuotos mokėjimo operacijos pasekmių ir pareiškėjo teisės į mokėjimo operacijų sumų grąžinimą

Pagal Mokėjimų įstatymo 38 straipsnio 1 dalį, mokėtojo mokėjimo paslaugų teikėjas privalo grąžinti mokėtojui neautorizuotos mokėjimo operacijos sumą ne vėliau kaip iki kitos darbo dienos nuo sužinojimo apie tokios mokėjimo operacijos įvykdymą, išskyrus atvejus, kai mokėtojo mokėjimo paslaugų teikėjas turi pagrįstų priežasčių įtarti mokėtojo sukčiavimą ir apie šias priežastis raštu praneša priežiūros institucijai (Lietuvos bankui).

Mokėjimų įstatymo 39 straipsnio 1 dalis nustato, kad mokėtojui gali tekti dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai iki 50 Eur, 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

---

2016 m. gegužės 12 d. nutartis civilinėje byloje Nr. 3K-3-268-421/2016).

neturi patirti jokių nuostolių, jeigu 1) jis iki mokėjimo operacijos įvykdymo negalėjo pastebėti mokėjimo priemonės praradimo, vagystės arba neteisėto pasisavinimo, išskyrus atvejus, kai jis veikė nesąžiningai; 2) nuostoliai yra patirti dėl mokėjimo paslaugų teikėjo, jo darbuotojo, tarpininko, filialo ar asmenų, kuriems perduotas veiklos funkcijų valdymas, veiksmų ar neveikimo.

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 šio straipsnio 1 dalyje nustatytas didžiausios nuostolių sumos ribojimas netaikomas."

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 (Mokėjimų įstatymo 34 straipsnio 2 dalis).

Mokėjimų įstatymas aiškiai nustato, kad tuo atveju, kai mokėtojas neigia autorizavęs įvykdytą mokėjimo operaciją, mokėtojo mokėjimo paslaugų teikėjo arba atitinkamais atvejais mokėjimo inicijavimo paslaugos teikėjo užregistruotas mokėjimo priemonės naudojimas nebūtinai yra pakankamas įrodymas, kad mokėtojas autorizavo mokėjimo operaciją ar veikė nesąžiningai arba tyčia ar dėl didelio neatsargumo neįvykdė vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų. Mokėtojo mokėjimo paslaugų teikėjas ir atitinkamais atvejais mokėjimo inicijavimo paslaugos teikėjas turi pateikti įrodymų, kuriais patvirtinamas mokėtojo sukčiavimas arba didelis neatsargumas (Mokėjimų įstatymo 37 straipsnio 3 dalis).

Įvertinus pirmiau nurodytas Mokėjimų įstatymo nuostatas, galima teigti, kad mokėtojo mokėjimo paslaugų teikėjas gali būti visiškai atleistas nuo pareigos grąžinti mokėtojui neautorizuotos mokėjimo operacijos sumą tik tuo atveju, jeigu pateikia įrodymų dėl mokėtojo sukčiavimo (nesąžiningumo arba tyčios) arba didelio neatsargumo (Mokėjimų įstatymo 37 straipsnio 3 dalis ir 39 straipsnio 3 dalis).

Aplinkybių ir duomenų, kaip ir šalių ginčo dėl to, kad pareiškėjas galėjo veikti nesąžiningai arba tyčia, nėra. Tai reiškia, kad, siekiant įvertinti, ar bankas pagrįstai atsisako kompensuoti pareiškėjo nuostolius, susijusius su mokėjimo operacijų įvykdymu, ir ar galėtų pareiškėjo atžvilgiu būti taikoma Mokėjimų įstatymo 39 straipsnio 3 dalis, būtina nustatyti, ar pareiškėjo elgesys, atskleidžiant personalizuotus jam išduotų mokėjimo priemonių požymius, taip pat kiti veiksmai, dėl kurių galėjo būti įvykdytos mokėjimo operacijos, vertintini kaip didelis pareiškėjo neatsargumas, dėl kurio visi jo reikalaujami atlyginti nuostoliai turėtų tekti pačiam pareiškėjui.

Lietuvos bankas, nagrinėdamas ginčus dėl nuostolių, susijusių su neautorizuotomis mokėjimo operacijomis, įvykusiomis dėl sukčiavimo atakų, ir spręsdamas dėl mokėjimo paslaugų teikėjo atsakomybės šiuos nuostolius atlyginti, nustačius, kad vartotojas (mokėtojas) jam teisės aktuose ir (ar) sutartyje nustatytas pareigas, susijusias su mokėjimo priemonėmis, vykdė netinkamai, elgdamasis labai neapdairiai, laikosi nuomonės, kad didelis neatsargumas yra vertinamojo pobūdžio aplinkybė. Tai reiškia, kad išvada dėl mokėtojo elgesio vertinimo kaip neatsargaus ar labai neatsargaus dėl neautorizuotos (-ų) mokėjimo operacijos (-ų) darytina kiekvienu konkrečiu atveju, įvertinus ginčo nagrinėjimo metu nustatytų individualių, specifinių aplinkybių visumą, kurią patvirtina ginčo byloje esantys įrodymai ir (arba) yra šalių neginčijamos neautorizuotos mokėjimo operacijos įvykdymo aplinkybės. Taigi, šiuo atveju išvada dėl pareiškėjo, kaip mokėtojo, paprasto ar didelio neatsargumo, kaip vertinamojo pobūdžio aplinkybė, negali būti daroma izoliuotai, neįvertinus viso mokėjimo operacijų įvykdymo ir su juo susijusių aplinkybių konteksto.

Bankas savo sprendimą nekompensuoti pareiškėjo nuostolių, be kita ko, grindžia pareiškėjo veiksmais, lėmusiais mokėjimo operacijų įvykdymą, kurie, banko vertinimu, rodo pareiškėjo didelį neatsargumą vertinamomis aplinkybėmis. Banko teigimu, pareiškėjas buvo labai neatsargus, nes suvedė tik jam žinomą interneto banko atpažinimo kodą ir savo asmens kodą trečiųjų asmenų sukurtoje interneto svetainėje, į kurią pateko paspaudęs SMS pranešime pateiktą nuorodą, kuri neatitinka banko interneto banko svetainės adreso ir kuri visiškai nesusijusi su banku ir jo naudojamais interneto adresais. Be to, pareiškėjas, atsiradus tai

padaryti raginantiems „Smart-ID" paskyros pranešimams mobiliajame telefone, suvedė ir šios savo naudojamos atpažinties priemonės PIN kodus. Bankas atkreipia dėmesį, kad pareiškėjas nuspaudė trečiųjų asmenų atsiųstą nuorodą, neįsitikinęs, ar ji atitinka banko interneto banko svetainės adresą, ir nors turėjo galimybę pasitikslinti, ar SMS pranešimą tikrai atsiuntė bankas, į banką nesikreipė ir pasirinko spausti neaiškią nuorodą, o vėliau, nors turėjo galimybę suprasti, kad pats neinicijuoja programėlės sukūrimo kitame įrenginyje ir naujų PIN kodų nekuria, pasirinko suvesti savo „Smart-ID" paskyros PIN2 kodą, taip patvirtindamas programėlės ir naujų PIN kodų sukūrimą trečiųjų asmenų įdiegtame įrenginyje.

Lietuvos bankas, siekdamas nustatyti, ar pareiškėjo elgesys vertinamų aplinkybių kontekste gali būti laikomas dideliu neatsargumu, mano, kad šiuo atveju svarbu nustatyti, kaip pareiškėjas buvo įtikintas atskleisti savo mokėjimo priemonės personalizuotus saugos bei kitus duomenis tam, kad, nesant pareiškėjo valios, būtų inicijuotos ir patvirtintos mokėjimo operacijos.

Remiantis kreipimesi pareiškėjo pateiktais paaiškinimais buvo nustatyta, kad 2022 m. rugpjūčio 6 d. pareiškėjas į savo mobilųjį telefoną banko vardu gavo trečiųjų asmenų siųstą SMS pranešimą, įspėjantį apie paskyros apribojimą ir raginantį spausti tame pačiame SMS pranešime pateiktą nuorodą. Ginčo byloje esančiais duomenimis, pareiškėjas paspaudė pranešime pateiktą nuorodą ir atsidariusiame interneto puslapyje suvedė savo interneto banko atpažinimo kodą, asmens kodą bei vėliau Smart-ID" paskyros PIN1 ir PIN2 kodus.

Remiantis banko pateiktais įrodymais[2], sukčių sukurtoje svetainėje įvedus tik pareiškėjui žinomus personalizuotus saugumo duomenis (atpažinimo kodą ir asmens kodą), pareiškėjo papildomai buvo prašoma patvirtinti savo tapatybę, suvedant tik pareiškėjui žinomą „Smart-ID" paskyros PIN1 kodą, ir patvirtinti prisijungimą prie savo banko paskyros („Smart-ID" lange buvo rodoma informacija – *Login to SEB*). Vėliau programėlei bei naujiems PIN kodams sukurti pareiškėjo buvo prašoma suvesti tik pareiškėjui žinomą „Smart-ID" paskyros PIN2 kodą („Smart-ID" lange buvo rodoma informacija – *kuriate naujus SEB programos PIN kodus. Patvirtinkite mobiliosios programėlės sukūrimą).*

Taigi, remiantis ginčo byloje esančiais įrodymais, pareiškėjui, prieš suvedant savo naudojamos „Smart-ID" paskyros PIN 2 kodą, atitinkamame „Smart-ID" programėlės pranešime buvo nurodyta, kokiu tikslu pareiškėjo tai prašoma padaryti. Pareiškėjas telefoninio pokalbio metu bankui teigė, kad prieš vesdamas „Smart-ID" paskyros PIN2 kodą matė informaciją, kad šiuo veiksmu tvirtina programėlės ir naujų PIN kodų sukūrimą, tačiau vis tiek prašomus veiksmus atliko, nors turėjo tikslą tik prisijungti prie savo interneto banko ir neturėjo tikslo sukurti programėlės ir naujų PIN kodų.

Kaip minėta, Mokėjimų įstatymo 34 straipsnyje reglamentuojama viena iš mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigų – naudotis mokėjimo priemone pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas. Banko Bendrųjų taisyklių 1 priedo 10 skyriuje nurodyta, kad banko suteiktą mokėjimo priemonę ir su ja susijusius personalizuotus saugumo duomenis mokėtojas privalo saugoti ir imtis visų reikiamų veiksmų, kad personalizuoti saugumo duomenys nebūtų atskleisti jokiems kitiems asmenims. Be to, remiantis banko Paslaugų interneto banke teikimo sąlygų aprašo nuostatomis, klientas įsipareigoja saugoti atpažinimo priemones, nedelsdamas informuoti banką apie šių priemonių praradimą ar slaptumo pažeidimą. Jei atpažinimo priemonių praradimas susijęs su trečiųjų asmenų neteisėtais veiksmais, tai klientas privalo apie tai nedelsdamas pranešti teisėsaugos institucijoms. Už atpažinimo priemonių saugojimą ir tinkamą naudojimą, neatskleidimą tretiesiems asmenims yra atsakingas klientas. Paslaugų interneto banke teikimo sąlygų aprašas, be kita ko, nustato, kad klientas įsipareigoja laikyti paslaptyje atpažinimo kodą, slaptažodžius, PIN kodus, neužrašyti jų ant generatoriaus ar kitų kartu su juo laikomų daiktų ir jokia kita forma neatskleisti ar nepadaryti jų prieinamų tretiesiems asmenims (20.4 ir 38 punktai).

Taigi, pirmiau aptartos banko Bendrųjų taisyklių ir Paslaugų interneto banke teikimo sąlygų aprašo nuostatos, nors ir nedetalizuoja tapatybės patvirtinimo priemonės „Smart-ID" bei jos PIN kodų suvedimo teisinės reikšmės mokėjimo nurodymų įvykdyti mokėjimo operacijas inicijavimo ir patvirtinimo procese, tačiau jos aiškiai ir nedviprasmiškai nustato, kad už tapatybės patvirtinimo priemonės personalizuotų saugumo duomenų konfidencialumą yra atsakingas mokėtojas, šiuo atveju – pareiškėjas.

Atsižvelgiant į tai, manytina, kad pareiškėjo elgesys būtų laikomas kaip atitinkantis

[2] Banko informacinių sistemų žurnalo duomenys.

mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, jei būtų nustatyta, kad pareiškėjas ėmėsi adekvačių veiksmų (ar 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.

Įvertinęs ginčo byloje esančius duomenis ir ginčo nagrinėjimo metu nustatytas aplinkybes, Lietuvos bankas vis dėlto mano, kad išvados, jog pareiškėjo elgesys atitiko banko nustatytas naudojimosi mokėjimo priemonėmis sąlygas ir buvo adekvatus, pakankamas tam, kad pareiškėjui nustatytos pareigos, susijusios su mokėjimo priemonių personalizuotų saugumo duomenų konfidencialumo užtikrinimu, būtų tinkamai įvykdytos, daryti negalima.

Visų pirma, kaip jau buvo konstatuota pirmiau, pareiškėjo ginčijamos mokėjimo operacijos buvo patvirtintos trečiųjų asmenų mobiliajame įrenginyje pareiškėjo vardu įdiegus programėlę. Kaip ir buvo nustatyta ginčo byloje, programėlės pareiškėjo vardu įdiegimą trečiųjų asmenų įrenginyje patvirtino pats pareiškėjas suvesdamas „Smart-ID" paskyros PIN2 kodą. Tokią išvadą dėl pareiškėjo elgesio kaip itin neapdairaus vertinimo aptariamų aplinkybių metu pagrindžia ir sustiprina pirmiau aptarta aplinkybė, kad „Smart-ID" pranešimas, kuriuo pareiškėjo buvo prašoma suvesti PIN2 kodą, kad būtų patvirtintas programėlės įdiegimas trečiųjų asmenų įrenginyje, pakankamai aiškiai ir nedviprasmiškai informavo pareiškėją, kokiu tikslu jo tai padaryti prašoma, t. y. kad suvedant PIN2 kodą bus tvirtinamas programėlės ir naujų PIN kodų sukūrimas. Pareiškėjas šią jam pateiktą informaciją matė ir, nors neturėjo tikslo sukurti programėlę, elgėsi labai neatsargiai ir vis tiek suvedė „Smart-ID" paskyros PIN2 kodą.

Sprendžiant dėl pareiškėjo neatsargumo laipsnio, taip pat būtina atkreipti dėmesį į tai, kad trečiųjų asmenų pareiškėjui siųsta SMS žinutė informavo pareiškėją, kad, kaip teigia pats pareiškėjas, jo „paskyra užblokuota". Lietuvos banko nuomone, SMS žinutė su nuoroda į galimai suklastotą banko interneto banko puslapį galėjo sukurti pirminį įspūdį, kad ji siųsta banko: ji buvo siųsta banko vardu, nuorodos pavadinime naudojamas banko pavadinimas. Kita vertus, svarbu ir tai, kad SMS žinutėje pateikta nuoroda į tariamą banko interneto banko svetainę *https://seb-ltsaskaita.net* visiškai neatitinka tikrosios banko interneto svetainės adreso[3] ir neturi jokių sąsajų su interneto banke teikiamomis paslaugomis ar raginimu imtis veiksmų paskyros apribojimui panaikinti.

Be to, kaip pagrindžia banko kartu su atsiliepimu pateikti duomenys, pareiškėjui prieš suvedant PIN2 kodą, jo naudojamos „Smart-ID" paskyros lange buvo rodoma informacija, kokiu tikslu pareiškėjo buvo prašoma minėtus veiksmus atlikti, taigi, kad šį kodą pareiškėjo prašoma suvesti ne tariamam paskyros apribojimui panaikinti.

Manytina, kad šios aplinkybės, kurios vidutiniškai apdairų ir rūpestingą vartotoją būtų privertusios sudvejoti dėl atliekamų veiksmų ir pateiktų prašymų pagrįstumo, pareiškėjui galėjo nesukelti jokių abejonių tik dėl to, kad vertinamų aplinkybių metu pareiškėjas buvo itin neatidus – prieš suvesdamas savo naudojamos „Smart-ID" paskyros PIN2 kodą, pareiškėjas nors ir perskaitė „Smart-ID" programėlės pranešimo tekstą, informavusį pareiškėją, kokiu tikslu jo prašoma suvesti šį kodą. Pareiškėjas ne tik paspaudė nuorodą į suklastotą banko interneto banko svetainę, atskleisdamas ten savo mokėjimo priemonių personalizuotus saugumo duomenis, bet perskaitęs bei neįvertinęs „Smart-ID" programėlės pranešimų teksto, aiškiai nurodžiusio prašomų atlikti veiksmų tikslą, suvedė „Smart-ID" paskyros PIN2 kodą.

Aptariamų aplinkybių kontekste įvertintina ir tai, kad, banko pateiktais duomenimis, banko interneto banko paslaugomis su mobiliajame telefone susikurta „Smart-ID" paskyra pareiškėjas naudojasi dar nuo 2018 m., tad tikrasis banko interneto banko svetainės adresas, kaip ir naudojimosi pačia „Smart-ID" programėle esminiai ypatumai (pavyzdžiui, kokiu tikslu gali būti prašoma suvesti „Smart-ID" PIN2 kodą ir kad šios programėlės pranešimuose, prašančiuose suvesti PIN kodus, įprastai rodoma ir (ar) gali būti rodoma informacija, kokiu tikslu prašoma tai atlikti) pareiškėjui turėjo būti žinomi.

Be to, bankas kartu su atsiliepimu Lietuvos bankui pateikė duomenis, kad yra siuntęs (pvz., 2022 m. gegužės 23 d.) įspėjamuosius pranešimus į pareiškėjo interneto banko paskyrą apie sukčių atakas su raginimu nespausti jokių siunčiamų aktyvių nuorodų. Bankas taip pat nurodo nuolat informuojantis savo klientus apie su sukčiavimu susijusias rizikas savo interneto svetainėje[4].

---

[3] https://www.seb.lt/privatiems/kasdiene-bankininkyste/nuotolines-paslaugos/interneto-bankas; https://e.seb.lt/web/ipank.p?lang=lit.

[4] Nusikaltėliai internete tobulėja. Ką gali nuveikti turėdami Jūsų duomenis? | SEB ; Telefoniniai sukčiai apsimeta ir kurjeriais: kada verta sunerimti? | SEB ; Nusikaltėliai internete tobulėja. Ką gali nuveikti turėdami Jūsų duomenis? | SEB ; https://www.seb.lt/infobankas/naujienos/gresme-savo-pinigams-galime-nesiotis-kiseneje-kaip-nuo-jos-

Kaip minėta pirmiau, išvada dėl mokėtojo elgesio vertinimo kaip neatsargaus ar labai neatsargaus dėl neautorizuotos mokėjimo operacijos darytina kiekvienu konkrečiu atveju, įvertinus ginčo nagrinėjimo metu nustatytų individualių, specifinių aplinkybių visumą, kurią patvirtina ginčo byloje esantys įrodymai ir (arba) yra šalių neginčijamos neautorizuotos mokėjimo operacijos įvykdymo aplinkybės. Vis dėlto šiuo atveju nustatytos ir pirmiau analizuotos aplinkybės, susijusios tiek su pačios sukčiavimo atakos pobūdžiu, tiek su banko veiksmais, o svarbiausia – susijusios su pačio pareiškėjo veiksmais, ir būtent šių aplinkybių visuma, nesudaro pagrindo vertinti pareiškėjo elgesio tik kaip neatsargaus.

Pareiškėjas kritiškai neįvertino gautos SMS žinutės turinio, paspaudė joje pateiktą nuorodą ir suklastotoje banko interneto svetainėje suvedė personalizuotus saugumo duomenis ir nedvejodamas suvedė savo „Smart-ID" paskyros PIN2 kodą tik todėl, kad nebuvo atsargus ir rūpestingas, kiek akivaizdžiai buvo būtina vertinamomis aplinkybėmis. Taigi, pareiškėjas ne tik netinkamai vykdė jam, kaip mokėtojui, Mokėjimų įstatyme nustatytas pareigas, susijusias su jai išduotomis mokėjimo priemonėmis ir jų personalizuotais saugumo duomenimis, bet ir darė tai elgdamasis labai neatsargiai.

Tai reiškia, kad pareiškėjo elgesys vertinamomis aplinkybėmis nebuvo toks, koks akivaizdžiai buvo būtinas, ir tai šiuo atveju lėmė, kad tretieji asmenys įgijo galimybę pareiškėjo vardu inicijuoti mokėjimo operacijas.

Konstatavus, kad pareiškėjas, nesilaikydamas jam, kaip mokėtojui, Mokėjimų įstatyme ir sutartyje su banku nustatytų pareigų, susijusių su jam 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) pareiškėjui neautorizuoto Mokėjimo lėšų.

Įvertinus visa tai, kas išdėstyta pirmiau, ir nustačius, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, darytina išvada, kad pareiškėjo bankui keliamas reikalavimas grąžinti ir (ar) kompensuoti pareiškėjui mokėjimo operacijų sumą 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 pareiškėjo 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 arba kitą ginčų nagrinėjimo instituciją 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

apsisaugoti .