



**LIETUVOS BANKO
TEISĖS IR LICENCIJAVIMO DEPARTAMENTO
DIREKTORIUS**

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

2022 m. rugsėjo 2 d. Nr. 429-424
Vilnius

Lietuvos bankas gavo Valstybinės vartotojų teisių apsaugos tarnybos persiūtą X. X. (toliau – pareiškėja) kreipimąsi, kuriuo prašoma išnagrinėti tarp pareiškėjos ir AB SEB banko (toliau – bankas) kilusį ginčą.

N u s t a t y t a:

Ginčo nagrinėjimo metu nustatytais duomenimis, pareiškėja 2022 m. gegužės 21 d. gavo SMS pranešimą su nuoroda. Paspaudus trečiųjų asmenų atsiūtą nuorodą, atsiradė netikras banko interneto puslapis, imituojantis banko interneto puslapį, kuriame buvo prašoma įvesti pareiškėjai asmeniškai suteiktus unikalius duomenis – interneto banko atpažinimo kodą ir asmens kodą, būtinus prisijungti prie interneto banko, ir pareiškėjos naudojamos atpažinties priemonės „Smart-ID“ paskyros PIN1 kodą. Suvedus minėtus duomenis, tretieji asmenys prisijungė prie pareiškėjos interneto banko paskyros ir jos vardu įdiegė banko mobiliąją programėlę trečiųjų asmenų kontroliuojamame įrenginyje (mobiliajame telefone). Naudodamiesi banko mobiliąja programėle, tretieji asmenys inicijavo 2 000 Eur vertės mokėjimą, kuris buvo patvirtintas suvedus pareiškėjos naudojamos atpažinties priemonės „Smart-ID“ paskyros PIN2 kodą (toliau – Mokėjimas).

2022 m. gegužės 21 d. 23.40 val. pareiškėja telefonu kreipėsi į banką, norėdama pranešti apie sukčiavimo atvejį. Telefoninio pokalbio metu banko darbuotoja blokavo pareiškėjos interneto banko paskyrą ir rekomendavo pareiškėjai dėl sukčiavimo kreiptis į teisėsaugos institucijas.

2022 m. gegužės 23 d. bankas kreipėsi į lėšų gavėjo mokėjimo paslaugų teikėją „Verse Payment Lithuania“ dėl Mokėjimo lėšų grąžinimo, tačiau lėšų gavėjo mokėjimo paslaugų teikėjas nepateikė bankui atsakymo dėl lėšų grąžinimo. Apie tai bankas informavo pareiškėją pranešimu interneto banko paskyroje.

Pareiškėja, ginčydama banko sprendimą nekompensuoti jos nuostolių dėl įvykdyto Mokėjimo, kreipėsi dėl ginčo nagrinėjimo. Kreipimesi pareiškėja teigia, kad Mokėjimas buvo įvykdytas dėl saugumo spragų banko sistemose, nes Mokėjimo suma iš pareiškėjos sąskaitos buvo nurašyta jai suvedus tik jos naudojamos „Smart-ID“ paskyros PIN1 kodą, nors apie tai (t. y. kad mokėjimo operacijai autorizuoti gali pakakti „Smart-ID“ paskyros PIN1 kodo suvedimo) pareiškėja, jos teigimu, banko nebuvo informuota. Kreipimesi pareiškėja prašo rekomenduoti bankui kompensuoti jai ginčijamo Mokėjimo sumą.

Bankas nesutinka tenkinti pareiškėjos reikalavimo.

Banko teigimu, pareiškėja nesilaikė jai su išduotomis mokėjimo priemonėmis susijusių pareigų, nustatytų teisės aktuose ir šalių sutartinius santykius reglamentuojančiuose dokumentuose. Bankas mano, kad pareiškėja elgėsi itin neapdairiai ir neatsargiai, nes: paspaudė neaiškiai nuorodą, suvedė savo interneto banko atpažinimo kodą, asmens kodą ir savo mobiliąjame įrenginyje savo atliekamus veiksmus patvirtino suvedama tik pareiškėjos žinioje esančios „Smart-ID“ paskyros PIN1 ir PIN2 kodus, dėl to tretieji asmenys galėjo ne tik pareiškėjos vardu inicijuoti Mokėjimą banko mobiliojoje programėlėje, bet ir ginčijamas Mokėjimas buvo tinkamai patvirtintas.

Bankas atsiliepiame pažymi, kad operacijoms tvirtinti bankas taiko papildomą kliento ir jo operacijų autentifikavimą, taip siekdamas suteikti galimybę klientui įsitikinti inicijuojamos operacijos teisėtumu – klientams įvykdžius visas būtinas sąlygas, sutartas tarp banko ir kliento, kuriomis yra tinkamai identifikuojama kliento inicijuota operacija, bankas įsipareigoja tokias

operacijas įvykdyti. Bankas nurodo, kad Mokėjimo vykdymo metu banko sistemos veikė saugiai, nebuvo užfiksuota jokių sutrikimų. Banko teigimu, Mokėjimas buvo įvykdytas, nes pareiškėja paspaudė nuorodą, kuri nuvedė į sukčių sukurtą interneto puslapį, suvedė tik jai žinomus personalizuotus duomenis, o vėliau ir savo naudojamos atpažinties priemonės („Smart-ID“ paskyros) PIN kodus, šitaip suteikdama galimybę sukčiams inicijuoti ir atlikti Mokėjimą. Banko teigimu, jis deda visas pastangas ir vykdo visus reikalavimus, kad užtikrintų klientų lėšų saugumą, tačiau neturi galimybės kontroliuoti klientų neatsargių veiksmų, kurie nėra ir negali būti banko kontroliuojami. Įvertinęs aplinkybių visumą ir teisinį reglamentavimą, bankas mano, kad neturi pareigos pareiškėjai kompensuoti nuostolių, patirtų dėl Mokėjimo įvykdymo.

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. Lietuvos bankas ginčo nagrinėjimo proceso metu neatlieka Lietuvos Respublikos Lietuvos banko įstatymo 42¹ straipsnyje reglamentuojamų patikrinimų, skirtų faktinėms aplinkybėms dėl Lietuvos banko prižiūrimo finansų rinkos dalyvio galimo Lietuvos banko kompetencijai priskirtų teisės aktų reikalavimų pažeidimo nustatyti ir įvertinti. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Pareiškėjos ir banko ginčas kilo dėl banko atsisakymo gražinti ir (arba) kompensuoti pareiškėjai jos ginčijamo Mokėjimo, įvykdyto dėl trečiųjų asmenų surengtos sukčiavimo atakos, sumą. Pareiškėja mano, kad Mokėjimo įvykdymą lėmė saugumo spragos banko sistemose, todėl bankas yra atsakingas dėl pareiškėjos nuostolių, atsiradusių įvykdžius Mokėjimą sukčių naudai. Bankas teigia, kad tretieji asmenys įgijo sąlygas inicijuoti Mokėjimą tik dėl to, kad pareiškėja dėl didelio neatsargumo atskleidė savo mokėjimo priemonių personalizuotus saugumo duomenis tretiesiems asmenims ir Mokėjimą patvirtino suvedusi savo naudojamos „Smart-ID“ paskyros PIN2 kodą, todėl Mokėjimo lėšų gražinti ir (arba) kompensuoti pareiškėjai 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.

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).

Šalių neginčijamomis aplinkybėmis, ginčijamas Mokėjimas buvo inicijuotas ir įvykdytas trečiųjų asmenų, jiems neteisėtu būdu sužinojus (pasisavinus) pareiškėjos mokėjimo priemonių personalizuotus saugumo duomenis ir juos panaudojus Mokėjimui inicijuoti ir įvykdyti. Akivaizdu, kad Mokėjimo inicijavimas ir patvirtinimas neatitiko pačios pareiškėjos valios, nors formaliai (išoriniais požymiais) ir sutapo su pareiškėjos ir banko sutarta sutikimo mokėjimo operacijoms davimo forma ir tvarka. Pareiškėjos nurodytos aplinkybės, kad Mokėjimas nėra pareiškėjos autorizuotas, bankas atsiliepime iš esmės neginčija, todėl šio ginčo nagrinėjimo metu Lietuvos bankas daro išvadą, kad Mokėjimas, atliktas nesant pareiškėjos valios, laikytinas neautorizuotu.

Dėl neautorizuotos mokėjimo operacijos pasekmių ir pareiškėjos teisės į Mokėjimo sumos gražinimą

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

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 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 didžiausias 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 gražinti 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 pareiškėja galėjo veikti nesąžiningai arba tyčia, nėra. Tai reiškia, kad, siekiant įvertinti, ar bankas pagrįstai atsisako kompensuoti pareiškėjos nuostolius, susijusius su Mokėjimo įvykdymu, ir ar galėtų pareiškėjos atžvilgiu būti taikoma Mokėjimų įstatymo 39 straipsnio 3 dalis, būtina nustatyti, ar pareiškėjos elgesys, atskleidžiant personalizuotus jai išduotų mokėjimo priemonių požymius, taip pat kiti veiksmai, dėl kurių galėjo būti įvykdytas Mokėjimas, vertintini kaip didelis pareiškėjos neatsargumas, dėl kurio visi jos reikalaujami atlyginti nuostoliai turėtų tekti pačiai pareiškėjai.

Lietuvos bankas, nagrinėdamas ginčus dėl nuostolių, susijusių su neautorizuotomis mokėjimo operacijomis, įvykusiomis dėl sukčiavimo atakų, ir sprenddamas dėl mokėjimo paslaugų teikėjo atsakomybės šiuos nuostolius atlyginti, nustačius, kad vartotojas (mokėtojas) jam teisės aktuose ir (arba) 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 pareiškėjos, kaip mokėtojos, paprasto ar didelio neatsargumo, kaip vertinamojo pobūdžio aplinkybė, negali būti daroma izoliuotai, neįvertinus viso Mokėjimo įvykdymo ir su juo susijusių aplinkybių konteksto.

Bankas savo sprendimą nekompensuoti pareiškėjos nuostolių grindžia pareiškėjos veiksmais, lėmusiais Mokėjimo įvykdymą, kurie, banko vertinimu, rodo pareiškėjos didelį neatsargumą vertinamomis aplinkybėmis. Taigi bankas mano, kad pareiškėja buvo labai neatsargi, nes suvedė tik jai žinomą interneto banko atpažinimo kodą, asmens kodą trečiųjų asmenų sukurtoje interneto svetainėje, į kurią pateko paspaudusi SMS pranešime pateiktą nuorodą, neatitinkančią banko interneto banko svetainės adresu, kuris visiškai nesusijęs su

banku ir jo naudojamais interneto adresais, o vėliau, atsiradus tai padaryti raginantiesiems „Smart-ID“ paskyros pranešimams mobiliajame telefone, suvedė ir šios savo naudojamos atpažinties priemonės PIN kodus. Bankas atkreipia dėmesį, kad pareiškėja nuspaudė trečiųjų asmenų atsiųstą nuorodą, neįsitikinusi, ar ji atitinka banko interneto svetainės adresą, ir nors turėjo galimybę pasitikslinti, ar SMS pranešimą tikrai atsiuntė bankas, į banką nesikreipė ir pasirinko spausti neaiškia nuorodą, o vėliau, nors turėjo galimybę suprasti, kad pati jokios mokėjimo operacijos neinicijuoja, pasirinko suvesti savo „Smart-ID“ paskyros PIN2 kodą, taip patvirtindama ginčijamą Mokėjimą.

Lietuvos bankas, siekdamas nustatyti, ar pareiškėjos elgesys vertinamų aplinkybių kontekste gali būti laikomas dideliu neatsargumu, mano, kad šiuo atveju svarbu nustatyti, kaip pareiškėja buvo įtikinta atskleisti savo mokėjimo priemonės personalizuotus saugos bei kitus duomenis tam, kad, nesant pareiškėjos valios, būtų inicijuotas ir patvirtintas Mokėjimas.

Ginčo nagrinėjimo metu nustatyta, kad pareiškėja į bendrą savo mobiliojo telefono iš banko gautų žinučių srautą gavo trečiųjų asmenų siųstą SMS pranešimą banko vardu: „SEB: Jusu paskyra apribota dėl paskyros problemos- <https://sebpavirtinti.com/>“. Remiantis ginčo nagrinėjimo metu nustatytomis aplinkybėmis, pareiškėja paspaudė pranešime pateiktą nuorodą ir suklastotame banko interneto puslapyje suvedė savo interneto banko atpažinimo kodą ir asmens kodą, o vėliau, telefone pasirodžius tai atlikti raginantiesiems pranešimams, ir savo naudojamos „Smart-ID“ paskyros PIN1 ir PIN2 kodus.

Vertinant pareiškėjos veiksmų atsargumo laipsnį nagrinjamų aplinkybių kontekste, svarbu pažymėti, kad ginčo šalių sutartinių santykių neatskiriama dalimi esančių banko Bendrųjų taisyklių sąlygose ar kituose šalių sutartinius santykius reguliuojančiuose dokumentuose nėra paaiškinama tapatybės patvirtinimo priemonės „Smart-ID“, jos PIN kodų suvedimo reikšmė mokėjimo operacijų vykdymo procese ir jų panaudojimo galimos pasekmės klientui. Taigi, ginčo byloje nėra duomenų, kad pareiškėja būtų koku nors būdu tinkamai supažindinta su informacija, kokius veiksmus, naudodamasi „Smart-ID“ programėle, ji gali atlikti ir kokie veiksmai bei kokiais atvejais, naudojantis šia tapatybės patvirtinimo priemone ir suvedant jos PIN kodus, sukelia atitinkamas teises pasekmes sutartiniuose santykiuose su banku. Tokia informacija plačiau atskleidžiama tik banko interneto svetainėje adresu <https://www.seb.lt/privatiems/el-bankininkyste/paslaugos-internetu/prisijungimo-priemones-smart-id-m-parasas>. Pateiktos nuorodos skiltyje „Smart-ID lygmenys ir galimybės“ nurodoma, kad „Smart-ID“ „gali būti naudojama norint saugiai prisijungti prie interneto banko, tvirtinti mokėjimus, naudotis trečiųjų šalių paslaugų teikėjų paslaugomis ir pasirašyti elektroninius dokumentus. Prilygsta elektroniniam parašui.“ Bankas, paaiškindamas klientų supažindinimo su programėlės „Smart-ID“ naudojimosi ypatumais procesą, papildomai nurodė, kad „Smart-ID“ programėlės kūrėjai savo interneto svetainėje šios atpažinties priemonės naudotojams pateikia informaciją, kurioje aiškiai nurodyta „Smart-ID“ PIN kodų ir veiksmų su programėle „Smart-ID“ reikšmė, t. y. kad PIN1 yra naudojamas tapatybei patvirtinti, o PIN2 yra skirtas elektroniniam parašui¹.

Kita vertus, nors ginčo byloje nėra duomenų, jog būtent bankas būtų asmeniškai supažindinęs pareiškėją su jos naudojamos tapatybės patvirtinimo priemonės „Smart-ID“ bei jos PIN kodų suvedimo reikšme tarp šalių susiklosčiusiuose sutartiniuose santykiuose, pati pareiškėja, dėstydamą aplinkybes, nurodo, kad mokėjimo operacijoms autorizuoti ji naudoja (t. y. suveda) „Smart-ID“ paskyros PIN2 kodą, tad manytina, kad jo reikšmė mokėjimo operacijų tvirtinimo procese pareiškėjai, pagal jos pačios pateiktus paaiškinimus, yra žinoma. Nors pareiškėja banko atžvilgiu keliamą reikalavimą ir grindžia tuo, kad jos nebuvo prašoma suvesti „Smart-ID“ paskyros PIN2 kodą, taigi kad Mokėjimas buvo įvykdytas pareiškėjai suvedus tik „Smart-ID“ paskyros PIN1 kodą, vis dėlto, pagal banko pateiktus įrodymus², pareiškėjai sukčių sukurtoje svetainėje įvedus tik jai žinomus personalizuotus duomenis (atpažinimo kodą ir asmens kodą), pareiškėjos buvo prašoma papildomai patvirtinti savo tapatybę tik jai žinomu „Smart-ID“ paskyros PIN1 kodu ir Mokėjimą patvirtinti, t. y. patvirtinti, kad Mokėjimo informacija (gavėjas, suma) yra teisinga, buvo prašoma įvesti tik pareiškėjai žinomą „Smart-ID“ PIN2 kodą. Bankas pateikė duomenis, kad Mokėjimas buvo patvirtintas būtent pareiškėjos naudojamos atpažinties priemonės – „Smart-ID“ paskyros PIN2 kodu. Tai reiškia, kad, remiantis ginčo byloje esančiais įrodymais, vien tik PIN1 kodo suvedimo Mokėjimui patvirtinti, kaip teigia pareiškėja, neužteko.

Kaip minėta, Mokėjimų įstatymo 34 straipsnyje įtvirtinta viena iš mokėjimo paslaugų

¹ <https://www.smart-id.com/lt/pagalba/duk/registracija/kam-yra-reikalingi-du-pin-kodai>.

² Banko informacinių sistemų žurnalo duomenys.

naudotojo, 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, pagal banko Paslaugų interneto banke teikimo sąlygų aprašo nuostatas, 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 paslapyje 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 – pareiškėja. 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 (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 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.

Visų pirma, kaip jau buvo konstatuota pirmiau, ginčo byloje turimais įrodymais, pareiškėjos ginčijamas Mokėjimas, priešingai nei teigia pareiškėja, buvo patvirtintas pačios pareiškėjos naudojamos „Smart-ID“ paskyros PIN1 ir PIN2 kodais. Tokią išvadą dėl pareiškėjos elgesio vertinimo aptariamų aplinkybių metu pagrindžia ir sustiprina ir tai, kad, pagal banko pateiktus jo informacinių sistemų žurnalo duomenis, pareiškėjai savo naudojamose „Smart-ID“ paskyroje suvedant PIN1 kodą buvo rodomas tekstas „Payment of 2000.00 EUR. After confirmation this payment will be done“³ (liet. „2000.00 EUR mokėjimas. Po patvirtinimo mokėjimas bus įvykdytas.“), o suvedant PIN2 kodą buvo rodomas tekstas „2000.00 EUR to account ***9021“ (liet. „2000.00 EUR į sąskaitą ***9021“). Taigi, „Smart-ID“ pranešimai, kuriais pareiškėjos buvo prašoma suvesti PIN1 ir PIN2 kodus, pakankamai aiškiai ir nedviprasmiškai informavo pareiškėją, kokiu tikslu jos tai prašoma padaryti, tačiau to pareiškėja nepastebėjo ir (arba) neįvertino tik dėl to, kad buvo labai neatsargi, naudodama savo pasirinktą atpažinties priemonę.

Sprendžiant dėl pačios pareiškėjos neatsargumo laipsnio, būtina atkreipti dėmesį į tai, kad trečiųjų asmenų pareiškėjai siūsta SMS žinutė, parašyta be lietuviškų rašmenų, informavo pareiškėją apie tai, kad „Jūsų paskyra apribota dėl paskyros problemos-<https://sebpavirtinti.com/>“. Nors pareiškėjai į mobilųjį telefoną atsiūsta SMS žinutė galėjo sukurti pirminį įspūdį, kad šis pranešimas išsiūstas banko, nes buvo siūstas banko vardu ir pakliuvo į bendrą kitų banko siūstų SMS žinučių srautą, tačiau aplinkybė, kad banko vardu siūsta žinutė nepateikė jokių paaiškinimų dėl pareiškėjos „paskyros apribojimo“ (taigi, nei kokia pareiškėjos paskyra, nei dėl kokių priežasčių apribota), nesukėlė jokių abejonių pareiškėjai ir ji, kaip matyti iš ginčo nagrinėjimo metu nustatytų aplinkybių, nedvejodama paspaudė žinutėje esančią nuorodą į suklastotą banko interneto banko svetainę. Be to, pareiškėja ne tik paspaudė trečiųjų asmenų siūstoje SMS žinutėje pateiktą nuorodą į netikrą banko interneto banko puslapį,

³ Remiantis „Smart-ID“ programėlės kūrėjų viešai skelbiama informacija, programėlės nustatymuose „Smart-ID“ programėlės naudotojai patys turi pasirinkti pageidaujamą kalbą, kuria bus rodomi programėlės pranešimai ir kita informacija. Jei nepasirenkama pageidaujama kalba arba pasirinkta kalba nepalaikoma programėlėje, kaip numatytoji kalba programėlėje naudojama anglų k.

bet ir nesuabejojusi nuorodos ir atsidariusio interneto puslapio patikimumu, taip pat nekvestionuodama pateiktų nurodymų pagrįstumo, atskleidė savo mokėjimo priemonių personalizuotus saugumo duomenis, o vėliau ir suvedė savo naudojamos „Smart-ID“ paskyros PIN1 ir PIN2 slaptažodžius, atsiradus tai padaryti raginanties „Smart-ID“ programėlės pranešimams.

Aptariamų aplinkybių kontekste įvertintina ir pati trečiųjų asmenų siųstoje SMS žinutėje pateikta nuoroda – <https://sebpavirtinti.com>. Nors joje ir matomas banko pavadinimas, vis dėlto ji nėra tapati ir neatitinka tikrosios banko interneto banko svetainės adreso⁴, o pagal banko pateiktus duomenis, banko interneto banko paslaugomis su mobiliajame telefone susikurta „Smart-ID“ paskyra pareiškėja naudojasi nuo 2019 m., tad tikrasis banko interneto banko svetainės adresas pareiškėjai turėjo būti žinomas. Manytina, kad šios aplinkybės, kurios vidutiniškai apdairų ir rūpestingą vartotoją būtų privertusios sudvejoti atliekamų veiksmų ir pateiktų prašymų pagrįstumu, pareiškėjai jokių abejonių galėjo nesukelti tik dėl to, kad vertinamų aplinkybių metu pareiškėja buvo itin neatidi.

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 ginčo nagrinėjimo metu nustatytos ir pirmiau analizuotos aplinkybės, susijusios tiek su pačios sukčiavimo atakos pobūdžiu, tiek su banko veiksmais, o svarbiausia – susijusios su pačios pareiškėjos veiksmais, ir būtent šių aplinkybių visuma nesudaro pagrindo vertinti pareiškėjos elgesio tik kaip neatsargaus. Pareiškėja kritiškai neįvertino gautos SMS žinutės turinio, paspaudė joje pateiktą nuorodą, suklastotoje banko interneto banko svetainėje suvedė personalizuotus saugumo duomenis ir nedvejodama suvedė savo „Smart-ID“ paskyros PIN kodus tik todėl, kad nebuvo atsargi ir rūpestinga tiek, kiek akivaizdžiai buvo būtina vertinamomis aplinkybėmis. Tokiu būdu pareiškėja ne tik netinkamai vykdė jai, kaip mokėtojai, Mokėjimų įstatyme nustatytas pareigas, susijusias su jai išduotomis mokėjimo priemonėmis ir jų personalizuotais saugumo duomenimis, bet ir darė tai elgdama labai neatsargiai. Tai reiškia, kad pareiškėjos elgesys vertinamomis aplinkybėmis nebuvo toks, koks akivaizdžiai buvo būtinas, ir tai šiuo atveju lėmė, kad tretieji asmenys įgijo galimybę pareiškėjos vardu inicijuoti Mokėjimą, kuriam patvirtinimas duotas pačiai pareiškėjai savo „Smart-ID“ paskyroje suvedus PIN2 kodą, neįvertinus „Smart-ID“ programėlės pranešimų turinio prasmės, taigi, neįvertinus ir nesudvejojus dėl tokio prašymo naudoti savo atpažinties priemonę pagrįstumo.

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 mokėtojai tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai. Dėl šios priežasties, Lietuvos banko vertinimu, bankas neturi pareigos gražinti (kompensuoti) pareiškėjai neautorizuoto Mokėjimo lėšų.

Dėl mokėtojo teisės atšaukti pateiktą mokėjimo nurodymą

Pareiškėja kreipimesi, be kita ko, teigia, kad nors ji paskambino į banką po 10 minučių nuo, kaip teigia pareiškėja, „Smart-ID“ paskyros PIN1 kodo suvedimo tam, kad Mokėjimas būtų sustabdytas, tačiau bankas jos prašymo sustabdyti (atšaukti) Mokėjimą neįvykdė.

Vertinant pareiškėjos galimybę atšaukti savo vardu pateiktus mokėjimo nurodymus, 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 nustatyta, kad, pasibaigus 1 dalyje nurodytam laikotarpiui, mokėjimo nurodymas gali būti atšauktas tik tuo atveju, kai dėl to susitaria mokėjimo paslaugų vartotojas ir atitinkamas mokėjimo paslaugų teikėjas, o šio straipsnio 2 dalyje numatytais atvejais būtinas ir gavėjo sutikimas. Mokėjimo paslaugų teikėjas gali imti komisinį atlyginimą už mokėjimo nurodymo atšaukimą, jeigu tai numatyta bendrojoje sutartyje. Taigi, pasibaigus Mokėjimų įstatymo 44 straipsnio 1 dalyje nurodytam terminui, mokėjimo nurodymas gali būti atšauktas tik dėl to susitarus vartotojui ir jo mokėjimo paslaugų teikėjui, todėl nurodytos galimybės (t. y. mokėjimo nurodymo atšaukimo) įtvirtinimas Mokėjimų įstatyme neturėtų būti vertinamas kaip

⁴ <https://e.seb.lt/web/ipank.p?lang=lit>.

priverstinis lėšų gražinimas mokėtojai, esant jo atitinkamam prašymui (pasibaigus 44 straipsnio 1 dalyje nurodytam terminui).

Banko Bendrųjų taisyklių 1 priedo 3 skyriuje nurodyta, kad sutikimas atlikti mokėjimo operaciją gali būti atšauktas iki mokėjimo nurodymo gavimo banke momento, o sutikimas atlikti atidėtas arba periodines mokėjimo operacijas – ne vėliau kaip iki darbo dienos, einančios prieš dieną, kurią sutarta atlikti mokėjimo operaciją, pabaigos.

Vis dėlto, ginčo byloje nustatytais duomenimis⁵, Mokėjimas buvo įvykdytas 2022 m. gegužės 21 d. 23.25 val., o pareiškėja į banką paskambino 23.40 val. Taigi, pagal ginčo bylos duomenis, Mokėjimas iš pareiškėjos sąskaitos banke buvo įvykdytas dar iki pareiškėjos skambučio į banką ir pranešimo apie mokėjimo priemonės praradimą bei neautorizuotą jos panaudojimą. Tai reiškia, kad nei Mokėjimų įstatyme, nei šalių susitarime (banko Bendrosiose taisyklėse) nurodytos sąlygos atšaukti mokėjimo nurodymą įvykdyti Mokėjimą nagrinėjamo ginčo atveju nebuvo nustatytos, t. y. pareiškėja į banką su prašymu atšaukti mokėjimo nurodymus įvykdyti Mokėjimą paskambino po to, kai sutikimas minėtai mokėjimo operacijai atlikti jau buvo duotas ir banko mokėjimo paslaugų teikimo sąlygose nurodytas terminas atšaukti mokėjimo nurodymus jau buvo praėjęs.

Dėl banko teikiamų mokėjimo paslaugų saugumo

Pareiškėja, grįsdama banko atžvilgiu keliamą reikalavimą dėl nuostolių, susijusių su Mokėjimo įvykdymu, kompensavimo, nurodo ir tai, kad banko sistemos, pareiškėjos vertinimu, nėra pakankamai saugios.

Kaip minėta, Lietuvos bankas ginčo nagrinėjimo metu neatlieka patikrinimų tam, kad nustatytų, ar nebuvo pažeisti finansų įstaigų veiklai keliami teisės aktų reikalavimai. Lietuvos bankas remiasi ginčo šalių pateiktais konkrečiais įrodymais, kurių pagrindu priima sprendimą. Atsižvelgiant į tai, būtina konstatuoti, kad ginčo byloje nėra duomenų, galinčių patvirtinti pareiškėjos nurodytą aplinkybę, jog banko sistemos nėra saugios, o įvykdydamas Mokėjimą bankas būtų pažeidęs finansų rinką reglamentuojančių teisės aktų reikalavimus.

Pateikdamas paaiškinimus dėl pareiškėjos teiginių, susijusių su banko sistemų saugumu, bankas pažymėjo, kad Mokėjimo vykdymo metu nebuvo užfiksuota banko sistemų sutrikimų ar sulėtėjimo, bankas taip pat negavo pranešimų iš „Smart-ID“ programėlės kūrėjų apie „Smart-ID“ programėlės veikimo sutrikimus.

Pažymėtina, kad vien aplinkybė, jog Mokėjimas buvo įvykdytas, kaip pareiškėja nurodo, sukčių naudai, savaime nepagrindžia aplinkybės, kad banko taikytos saugumo priemonės net ir tuo atveju, jei būtų nustatyta, kad pareiškėja elgėsi itin apdairiai su jai išduotomis mokėjimo priemonėmis ir jų personalizuotais saugumo duomenimis, šiuo konkrečiu atveju buvo ne tik nepakankamos, bet ir neatitinkančios teisės aktų reikalavimų, ir tai galėjo nulemti Mokėjimo įvykdymą, dėl ko galėtų kilti ir atitinkama banko civilinė atsakomybė šių mokėjimų nulemtus nuostolius pareiškėjai kompensuoti. Kaip minėta, duomenų, kad bankas būtų nevykdęs finansų rinką reglamentuojančių teisės aktų reikalavimų, ginčo nagrinėjimo metu nenustatyta, savo deklaratyvių teiginių, kad banko sistemos nesaugios, jokiais duomenimis nepagrindė ir pati pareiškėja. Priešingai, įvertinus ginčo nagrinėjimo metu nustatytas aplinkybes, padaryta išvada, kad pareiškėjos nuostolius dėl Mokėjimo įvykdymo, prieš tai tretiesiems asmenims pasisavinus pareiškėjos mokėjimo priemonių personalizuotus saugumo duomenis, šiuo konkrečiu atveju nulėmė būtent pačios pareiškėjos itin neatsargūs veiksmai.

Todėl, įvertinus visa tai, kas išdėstyta pirmiau, ir nustačius, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, darytina išvada, kad pareiškėjos banko atžvilgiu keliamas reikalavimas gražinti pareiškėjai Mokėjimo lėšas 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.

⁵ Banko kartu su atsiliepimu pateikti banko informacinių sistemų žurnalo duomenys, pagal kuriuos matyti, kad sutikimas vykdyti Mokėjimą, suvedant pareiškėjos naudojamos „Smart-ID“ paskyros PIN2 kodą, duotas 2022 m. gegužės 21 d. 23.25 val., ir, kaip nurodo bankas, Mokėjimas, kaip momentinis mokėjimas, buvo įvykdytas ne ilgiau kaip per 10 sekundžių nuo sutikimo dėl jo davimo momento.

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