LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

SPRENDIMAS DĖL X. X. IR „SWEDBANK", AB, GINČO NAGRINĖJIMO

2022 m. liepos 8 d. Nr. 429-293
Vilnius

Lietuvos bankas gavo X. X. (toliau – pareiškėjas) kreipimąsi, kuriuo prašoma išnagrinėti pareiškėjo ir „Swedbank", AB, (toliau – bankas) ginčą.

N u s t a t y t a:

2021 m. rugsėjo 1 d. 19:05:12 val. pareiškėjo vardu baigta kurti nauja tapatybės patvirtinimo priemonė – „Smart-ID" paskyra Nr. (*duomenys neskelbtini*) (toliau – Paskyra Nr. 2). Sutikimas sukurti Paskyrą Nr. 2 duotas pareiškėjo įprastai naudojamame įrenginyje („Samsung Galaxy A51") susikurtos „Smart-ID" paskyros Nr. (*duomenys neskelbtini*) (toliau – Paskyra Nr. 1) taikomu PIN 2 slaptažodžiu. Tos pačios dienos 19:09:19 val. pareiškėjo vardu atidarytoje kredito limito sąskaitoje Nr. (*duomenys neskelbtini*) (toliau – Sąskaita) įvykdytas 2 150 Eur kredito pervedimas SEPA lėšų gavėjai Y.Y. į Revolut Payments, UAB, esančią jos sąskaitą (toliau – Gavėjo sąskaita)[1], mokėjimo paskirtyje nurodant „2372643" (toliau – Operacija). Operacijos lėšos iš Sąskaitos nurašytos ir šis kredito pervedimas kaip momentinis mokėjimas 19:09:22 val. perduotas Lietuvoje veikiančiam lėšų gavėjo mokėjimo paslaugų teikėjui.

2021 m. rugsėjo 1 d. 19:10 val. pareiškėjas bandė paskambinti Estijos įmonės „SK ID Solution AS", Lietuvoje veikiančios per savo filialą (toliau – „Smart-ID" kūrėjai), telefonu + 370 670 41 807. Tos pačios dienos 19:48 val. ir 20:13 val. pareiškėjas paskambino į banką telefonu, informavo apie gautas SMS žinutes, galbūt įvykusį sukčiavimo atvejį ir paprašė blokuoti jo mokėjimo priemones. Antrojo pokalbio su pareiškėju metu banko darbuotoja, gavusi pareiškėjo pranešimą apie Operaciją, 20:32:47 val. blokavo pareiškėjui prisijungti prie interneto banko išduotą naudotojo numerį (taip buvo užblokuota pareiškėjui teikiama interneto banko paslauga), iš „Smart-ID" duomenų bazės per banko informacinę sistemą 20:29:49 val. pašalino (ištrynė) Paskyrą Nr. 2, o 20:29:49 val. – Paskyrą Nr. 1[2].

Gavęs pareiškėjo pranešimą apie neautorizuotą Operaciją, bankas kitą darbo dieną 07:21:24 val. išsiuntė sisteminį SEPA atšaukimo pranešimą lėšų gavėjo mokėjimo paslaugų teikėjui Revolut Payments, UAB, ir tą pačią dieną 08:52:29 val. gavo atsakymą, kad lėšų Gavėjo sąskaitoje jau nėra, todėl nėra galimybės atšaukti Operacijos mokėtojo prašymu.

2021 m. rugsėjo 9 d. pareiškėjas interneto banko žinute kreipėsi į banką, prašydamas pateikti visų 2021 m. rugsėjo 1 d. vykusių jo pokalbių su banko darbuotojais garso įrašus.

Atsakydamas į pareiškėjo prašymą bankas 2021 m. rugsėjo 27 d. rašte Nr. (*duomenys neskelbtini*) pateikė informaciją apie Operacijos įvykdymo aplinkybes, 2021 m. rugsėjo 1 d. pokalbių su banko darbuotojais stenogramas ir atsisakymo atlyginti su Operacijos įvykdymu susijusių pareiškėjo nuostolių motyvus.

2021 m. spalio 14 d. pareiškėjas pakartotinai kreipėsi į banką, prašydamas atlyginti su Operacijos įvykdymu susijusius nuostolius. Į šią pareiškėjo pretenziją bankas atsakė 2021 m. spalio 28 d. raštu Nr. (*duomenys neskelbtini*), nurodydamas, kad sprendimo negrąžinti ir (ar) nekompensuoti pareiškėjui Operacijos lėšų bankas nekeis.

Pareiškėjas, nesutikdamas su banko sprendimu negrąžinti ir (ar) nekompensuoti jam

---

[1] 19:09:22 val. kredito pervedimo lėšos išsiųstos į lėšų gavėjo banką.

[2] Bankas atsiliepime papildomai nurodė, kad Operacijos įvykdymo dieną pareiškėjo įrenginyje sukurta paskyra Nr. (*duomenys neskelbtini*) (toliau – Paskyra Nr. 3) nebuvo naudojama ir buvo pašalinta 19:22:49 val., t. y. dar prieš pareiškėjui susisiekiant su banku telefonu. Paskyrą Nr. 3 pašalino ne banko darbuotojai, o „Smart-ID" kūrėjų atstovai.

Operacijos sumos, kreipėsi į Lietuvos banką. Kreipimesi pareiškėjas nurodė, kad 2021 m. rugsėjo 1 d. būdamas užsienyje į telefoną gavo SMS žinutę, kad jo „Smart-ID" paskyra užblokuota dėl saugumo. Praėjus 10 min. nuo nesėkmingo bandymo prisijungti prie savo interneto banko, pareiškėjas elektroniniu paštu iš banko gavo pranešimą, kad jo vardu sukurta nauja „Smart-ID" paskyra. Pareiškėjas iškart paskambinęs laiške nurodytu telefonu į banką pranešti, kad naujos „Smart-ID" paskyros nekūrė, ir paprašė ją užblokuoti. Praėjus 17 min. nuo gauto elektroninio laiško apie naujos „Smart-ID" paskyros sukūrimą, pareiškėjas gavo iš banko kitą laišką, kad naujoji paskyra užblokuota. Tada jis prisijungė prie savo interneto banko ir pamatė, kad sukurtas 2 500 Eur pervedimo ruošinys, nors jo sąskaitose lėšų jau nebuvo. Tada jis vėl paskambinęs elektroniniame laiške nurodytu telefono numeriu į banką ir banko darbuotoja jam pranešė, kad naujoji „Smart-ID" paskyra dar neužblokuota ir tai reikia padaryti kuo skubiau. Pareiškėjo teigimu, praėjus 11 min. nuo pirmojo pranešimo apie naujos „Smart-ID" paskyros užblokavimą, jis gavo kitą elektroninį laišką iš banko, kad naujoji „Smart-ID" paskyra užblokuota.

Pareiškėjui kelia abejonių tai, kad bankui nekilo įtarimų, jog naujoji „Smart-ID" paskyra sukurta ne iš pareiškėjo telefono aparato ir ne iš pareiškėjo numerio, taip pat tai, kad po pirmojo pokalbio su banko darbuotoja ši paskyra nebuvo užblokuota (nors elektroniniu laišku buvo pranešta, kad užblokuota). Pareiškėjo vertinimu, tai sudarė palankias sąlygas tretiesiems asmenims atlikti veiksmus jo Sąskaitoje, todėl jis prašė atlyginti dėl įvykdytos Operacijos patirtus nuostolius.

Nesutikdamas keisti savo sprendimo nekompensuoti ginčijamos Operacijos sumos bankas pažymėjo, kad ir pareiškėjo ginčijama Operacija, ir prieš tai atliktas mokėjimas iš vienos sąskaitos į kitą pareiškėjo sąskaitą banke buvo atlikti iš pareiškėjui nebūdingo įrenginio, todėl ginčo dėl to, ar šie mokėjimai laikytini pareiškėjo autorizuotais, nėra[3]. Bankas nurodė, kad sutikimas Operacijai duotas su pareiškėjo vardu sukurta Paskyra Nr. 2, o tai reiškia, kad tokiais atvejais, kai jungiamasi iš klientui nebūdingo įrenginio, būtina suvesti ne tik naudotojo ID numerį, bet ir asmens kodą. Dėl to, banko nuomone, atsitiktinis prisijungimas prie pareiškėjui teikiamos banko interneto banko paslaugos nėra galimas. Aplinkybę, kad pareiškėjo naudotojo ID numeris ir asmens kodas tapo žinomi tretiesiems asmenims būtent dėl pareiškėjo kaltės, pasireiškusios dideliu neatsargumu, patvirtina ir pareiškėjo pateikta iš nežinomo numerio ((*duomenys neskelbtini*)), kuris niekaip negali būti susijęs nei su banku, nei su „Smart-ID" kūrėjais, 2021 m. rugsėjo 1 d. gauto SMS pranešimo ekrano vaizdo kopija. Kokiu tiksliai laiku pareiškėjas gavo šį SMS pranešimą, nežinoma, nes ekrano vaizdo kopijoje nematyti minučių, o tik valanda, t. y. 18. Pranešime nurodyta, kad užblokuota pareiškėjo turima „Smart-ID" paskyra ir siūloma ją atsiblokuoti paspaudus aktyvią nuorodą, tačiau nežinoma, koks konkretus turinys buvo rodomas atsidariusiame netikrame interneto puslapyje ir koks to interneto puslapio tikrasis adresas, nes pareiškėjas sąmoningai tai nutylėjo. Lietuvos bankui adresuotame skunde šios aplinkybės pareiškėjas nekomentavo, o bankui apskritai neigė, kad pats atliko tokius veiksmus. Lietuvos bankui atsiųstame pareiškėjo susirašinėjime elektroniniu paštu su „Smart-ID" kūrėjais nurodyta, kad pareiškėjas pripažįsta paspaudęs tą nuorodą. Paspaudus gautame SMS pranešime buvusią aktyvią nuorodą, atsidarė interneto puslapis, kuriame buvo pateikti nurodymai, kurių pareiškėjas, banko manymu, nevertino kritiškai ir suvedė savo asmens duomenis (naudotojo ID numerį ir asmens kodą). Taip pareiškėjas tretiesiems asmenims perdavė tapatybei identifikuoti būtinus duomenis, kuriuos jie panaudojo suvesdami į tikrą interneto svetainę, kad įsidiegtų į savo valdomą išmanųjį telefoną pareiškėjo vardu „Smart-ID" programėlę. Bankas atkreipė dėmesį, kad pareiškėjo patirtis naudojantis banko teikiamomis elektroninėmis paslaugomis ir „Smart-ID" kaip tapatybės patvirtinimo priemone tuo metu buvo pakankama, nes pirmoji iš turimų „Smart-ID" paskyrų jam buvo sukurta dar 2018 m. kovo 18 d.[4]

Bankas pažymėjo, kad Operacija buvo įvykdyta kaip momentinis mokėjimas, tad jos atšaukti pareiškėjo dar pirmojo kreipimosi į banką metu nebuvo techniškai įmanoma, nes lėšos jau buvo išsiųstos į gavėjo banką ir gali būti, kad pareiškėjo pirmojo kreipimosi į banką metu Operacijos lėšų Gavėjo sąskaitoje jau nebuvo.

---

[3] Atsiliepime nurodyta, kad pareiškėjo vardu sutikimą Operacijai Sąskaitoje įvykdyti davė tretieji asmenys, panaudodami turimą įrenginį, kurio IP adresas, slapukas ir naršyklės duomenys pareiškėjo įprastai naudojamam įrenginiui nebuvo būdingi.

[4] Bankas paaiškino, kad pareiškėjas banko teikiama banko interneto banko paslauga su naudotojo ID numeriu (*duomenys neskelbtini*) naudojasi nuo tada, kai 2012 m. balandžio 25 d. su banku sudarė elektroninių paslaugų teikimo sutartį Nr. (*duomenys neskelbtini*) (toliau – Sutartis). Nuo 2021 m. rugsėjo 8 d. galioja nauja Sutarties specialiųjų sąlygų redakcija, pagal kurią klientui suteiktas naujas naudotojo ID numeris – (*duomenys neskelbtini*).

Banko nuomone, pareiškėjas Lietuvos bankui pateiktuose dokumentuose neginčijo aplinkybių, susijusių su dideliu neatsargumu duodant sutikimą Paskyrai Nr. 2 jo vardu trečiųjų asmenų valdomame įrenginyje sukurti. Banko teigimu, pareiškėjo labai neatsargūs veiksmai pažeidžiant jam kaip mokėtojui su mokėjimo priemonės naudojimu nustatytas pareigas, kai gavo iš trečiųjų asmenų SMS pranešimą, lėmė, kad tretieji asmenys pasisavino jo tapatybę, sukurdami kitame įrenginyje naują tapatybės patvirtinimo priemonę (Paskyrą Nr. 2), ir ja inicijavo visus pareiškėjo ginčijamus veiksmus, susijusius su prisijungimu prie jo interneto banko aplinkos, o vėliau įvykdė Operaciją. Banko vertinimu, net ir paspaudęs SMS pranešime esančią nuorodą ir suklastotoje banko interneto svetainėje suvedęs savo mokėjimo priemonių personalizuotus saugumo duomenis, pareiškėjas turėjo galimybę išvengti nuotolių, jei būtų perskaitęs savo naudojamo įrenginio ekrane rodomą informaciją apie tai, kokiam veiksmui prašoma duoti sutikimą suvedant Paskyros Nr. 1 PIN2 kodą.

Atsižvelgdamas į tai, kad pareiškėjas kartu su kreipimusi Lietuvos bankui pridėjo ir su „Swedbank" grupei priklausančia įmone sudarytą draudimo sutartį, bankas paaiškino, jog indėlių ir įsipareigojimų draudimo apsauga, kurią teikia VĮ „Indėlių ir investicijų draudimas", pareiškėjo atveju negali būti taikoma, nes šios draudimo apsaugos objektas yra Lietuvos kredito įstaigose laikomos indėlininkų lėšos bet kuria valiuta iki 100 000 Eur sumos, o pati draudimo apsauga galioja tais atvejais, kai kredito įstaiga yra nepajėgi įvykdyti savo finansinių įsipareigojimų indėlininkams dėl paskelbto kredito įstaigos bankroto, nemokumo ir kt. atvejais. Bankas nurodė, kad su Swedbank P&C Insurance AS Lietuvos filialu sudaryta kredito kortelės įsipareigojimų draudimo sutartis netaikoma nuotoliams dėl neautorizuotų mokėjimo operacijų su kredito kortele susietoje kredito limito sąskaitoje atlyginti. Šioje sutartyje draudimo objektas yra pareiškėjo kaip draudėjo turtiniai interesai, susiję su negalėjimu grąžinti panaudoto kredito tapus nedarbingu, bedarbiu dėl draudžiamojo įvykio.

Remdamasis atsiliepime išdėstytais argumentais bankas mano, kad jo veiksmai teikiant mokėjimo paslaugas Sąskaitoje, blokuojant pareiškėjo mokėjimo priemones ir įvykdant Operaciją buvo teisėti ir pagrįsti, todėl jis nepažeidė nei su pareiškėju sudarytų sutarčių sąlygų, nei įstatymų reikalavimų. Banko vertinimu, dėl pareiškėjo neautorizuotos Operacijos kilusius nuostolius jis pagrįstai atsisakė atlyginti vadovaudamasis teisės aktų nuostatomis, todėl prašo atmesti pareiškėjo 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.

Ginčas kilo dėl to, kad bankas atsisakė grąžinti ir (ar) kompensuoti pareiškėjui Operacijos, įvykdytos pareiškėjo vardu tretiesiems asmenims sukūrus naują „Smart-ID" paskyrą (Paskyrą Nr. 2) trečiųjų asmenų kontroliuojamame įrenginyje, sumos. Pareiškėjas mano, kad bankas nesiėmė tinkamų veiksmų, kad būtų laiku užblokuota Paskyra Nr. 2, ir tai sudarė sąlygas įvykdyti Operaciją sukčių naudai. Bankas teigia, kad tretieji asmenys įgijo sąlygas inicijuoti ir patvirtinti Operaciją tik dėl to, kad pareiškėjas dėl didelio neatsargumo atskleidė savo mokėjimo priemonių personalizuotus saugumo duomenis tretiesiems asmenims ir naujos „Smart-ID" paskyros (Paskyros Nr. 2) sukūrimą patvirtino suvesdamas savo naudojamos „Smart-ID" paskyros (Paskyros Nr. 1) PIN kodus, todėl neprivalo pareiškėjui grąžinti ir (ar) kompensuoti Operacijos lėšų.

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).

Šalys neginčija aplinkybių, kad Operacija buvo inicijuota ir įvykdyta trečiųjų asmenų,

jiems neteisėtu būdu sužinojus (pasisavinus) pareiškėjo mokėjimo priemonių personalizuotus saugumo duomenis ir juos panaudojus naujai „Smart-ID" paskyrai (Paskyrai Nr. 2) pareiškėjo vardu sukurti, o vėliau ir pačiai Operacijai inicijuoti ir įvykdyti. Akivaizdu, kad Operacijos inicijavimas ir patvirtinimas neatitiko pareiškėjo valios, nors formaliai (pagal išorinius požymius) ir sutapo su jo ir banko sutarta sutikimo mokėjimo operacijoms davimo forma ir tvarka. Bankas atsiliepime neginčija pareiškėjo nurodytos aplinkybės, kad jis neautorizavo Operacijos, todėl Lietuvos bankas daro išvadą, kad Operacija, atlikta nesant pareiškėjo valios ir jam net nežinant apie jos inicijavimo aplinkybę bei neišreiškus jokių valinių veiksmų jai patvirtinti, laikytina neautorizuota.

Dėl neautorizuotos mokėjimo operacijos pasekmių ir pareiškėjo teisės į Operacijos sumos 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 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 nustatytos šios 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 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 Operacijos įvykdymu, ir ar pareiškėjui galėtų 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 įvykdyta Operacija, vertintini kaip didelis neatsargumas, dėl kurio visi reikalaujami atlyginti nuostoliai turėtų tekti pačiam pareiškėjui.

Antrosios mokėjimo paslaugų direktyvos preambulės 72 punkte rašoma, kad siekiant įvertinti galimą mokėjimo paslaugų vartotojo aplaidumą ar didelį aplaidumą, reikėtų atsižvelgti

į visas aplinkybes. Įtariamo aplaidumo įrodymai ir laipsnis paprastai turėtų būti vertinami pagal nacionalinę teisę. Tačiau nors aplaidumo sąvoka reiškia, kad pažeidžiamas įsipareigojimas elgtis rūpestingai, didelis aplaidumas turėtų reikšti daugiau nei vien aplaidumą ir apimti labai nerūpestingą elgesį; pavyzdžiui, tai būtų mokėjimo operacijos autorizavimui naudojamų saugumo požymių laikymas prie mokėjimo priemonės atviru ir trečiosioms šalims lengvai atskleidžiamu formatu. Didelio neatsargumo sąvoka plėtojama ir Lietuvos Aukščiausiojo Teismo praktikoje. Kasacinis teismas yra išaiškinęs, kad didelis neatsargumas kaip kaltės forma pasireiškia neprotingu arba išskirtiniu rūpestingumo nebuvimu, kai asmuo nėra tiek rūpestingas, kiek akivaizdžiai būtina esamomis aplinkybėmis.[5]

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, 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) 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, t. y. išsamiai neįvertinus viso Operacijos įvykdymo ir su tuo susijusių aplinkybių konteksto.

Bankas savo sprendimą nekompensuoti pareiškėjo nuostolių grindė pareiškėjo veiksmais, lėmusiais Operacijos įvykdymą. Šie veiksmai, banko vertinimu, rodo pareiškėjo didelį neatsargumą vertinamomis aplinkybėmis. Taigi bankas teigia, kad pareiškėjo labai neatsargūs veiksmai, kuriais jis pažeidė savo kaip mokėtojo su mokėjimo priemonės naudojimu susijusias pareigas, lėmė, kad tretieji asmenys pasisavino jo tapatybę, sukurdami kitame įrenginyje naują tapatybės patvirtinimo priemonę (Paskyrą Nr. 2), ir ja inicijavo visus pareiškėjo ginčijamus veiksmus, susijusius su prisijungimu prie jo interneto banko aplinkos, o vėliau ir įvykdė Operaciją.

Vertinamų aplinkybių kontekste būtina pažymėti, kad remiantis nurodytų Mokėjimų įstatymo nuostatų analize mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai tik tuo atveju, jei tenkinamos abi sąlygos, t. y. mokėtojas ne tik neįvykdo vienos ar kelių jam Mokėjimų įstatyme nustatytų pareigų, bet ir padaro tai elgdamasis nesąžiningai arba tyčia ar būdamas labai neatsargus. Taigi banko sprendimas nekompensuoti pareiškėjo nuostolių dėl neautorizuotos Operacijos įvykdymo galėtų būti vertinamas kaip pagrįstas tik tuo atveju, jei būtų įrodyta, kad pareiškėjas, atskleisdamas personalizuotus savo mokėjimo priemonių saugumo duomenis ir taip sudarydamas galimybę tretiesiems asmenims panaudoti šiuos duomenis „Smart-ID" Paskyrai Nr. 2 sukurti, o vėliau ir inicijuoti bei patvirtinti Operaciją, elgėsi itin aplaidžiai, t. y. buvo labai neatsargus.

Lietuvos bankas, siekdamas nustatyti, ar pareiškėjo elgesys gali būti laikomas dideliu neatsargumu, vertino pareiškėjo pasitikėjimą į mobilųjį telefoną gautame SMS pranešime nurodyta informacija ir pateikta nuoroda, veiksmus, kuriais buvo sudarytos sąlygos tretiesiems asmenims sukurti naują „Smart-ID" paskyrą trečiųjų asmenų kontroliuojamame įrenginyje, taip pat banko veiksmus, kurių jis prevenciškai ėmėsi ir imasi tam, kad pareiškėjas būtų tinkamai supažindintas su sukčiavimo elektroninėje erdvėje rizikomis, tapatybės patvirtinimo priemonės saugaus naudojimo, personalizuotų saugumo žymenų suvedimo ir atskleidimo reikšme bei teisinėmis pasekmėmis.

Vertinant pareiškėjo elgesį svarbu nustatyti, kaip jis buvo įtikintas atskleisti savo mokėjimo priemonės personalizuotus saugumo ir kitus duomenis, kad būtų sukurta „Smart-ID" Paskyra Nr. 2, sudariusi sąlygas tretiesiems asmenims be pareiškėjo žinios ir valinių veiksmų inicijuoti ir patvirtinti Operaciją.

Ginčo nagrinėjimo metu nustatyta, kad pareiškėjas į savo mobilųjį telefoną gavo tokio turinio trečiųjų asmenų siųstą SMS pranešimą apie „Smart-ID" programėlės užblokavimą ir raginimą spausti tame pačiame pranešime pateiktą nuorodą: *„SmartID" programa uzblokuota del saugumo. Noredami to isvengti, spustelekite nuoroda: HK27346.info*". Kaip kreipimesi teigė pareiškėjas, gavęs šią žinutę, jis bandė prisijungti prie savo interneto banko, tačiau to padaryti

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

nepavyko, o po 10 minučių iš banko gavo elektroniniu paštu pranešimą, kad jo vardu sukurta nauja „Smart-ID" paskyra.

Ginčo byloje esančiais duomenimis, tretiesiems asmenims dar neužbaigus Paskyros Nr. 2 sukūrimo (užbaigta kurti 19:05:12 val.), bankas 19:01:54 val. suformavo SMS pranešimą, o 19:02 val. gavo atsakymą iš banko pasitelkto telekomunikacinių paslaugų teikėjo, kad į pareiškėjo bankui nurodytą telefono numerį pristatytas tokio turinio įspėjimas: „New Smart-ID account has been created. If it was not done by you - please call us immediately to 1884 or + 370 5 268 4444!". Iš viso bankas 2021 m. rugsėjo 1 d. pareiškėjui siuntė tokio turinio SMS pranešimus: 19:01:54 val. – „New Smart-ID account has been created. If it was not done by you - please call us immediately to 1884 or + 370 5 268 4444!"; 20:32:47 val. – „Jūsų interneto banko paskyra užblokuota".

Remiantis atsiliepime nurodytomis aplinkybėmis, trečiųjų asmenų valdomame įrenginyje pareiškėjo vardu sukurta nauja tapatybės patvirtinimo priemonė, t. y. Paskyra Nr. 2, buvo baigta kurti 19:05:12 val., kai tretieji asmenys prisijungė prie šios paskyros savo įrenginyje ir užbaigė visą kūrimo procesą. Bankas pareiškėją nedelsiant (19:02 val.) įspėjo, kai gavo informaciją apie pareiškėjo Paskyra Nr. 1 duotą sutikimą. „Smart-ID" kūrėjai elektroniniu paštu 19:05 val. taip pat įspėjo pareiškėją apie Paskyros Nr. 2 sukūrimą. Nuo banko SMS pranešimo ir „Smart-ID" kūrėjų elektroninio laiško pareiškėjui iki Operacijos Sąskaitoje autorizavimo pareiškėjo vardu momento buvo likę daugiau kaip 4 minutės.

Lietuvos bankas paprašė pareiškėjo papildomai paaiškinti, kokius duomenis jis nurodė, paspaudęs SMS pranešime pateiktą nuorodą atsidariusioje interneto svetainėje, ir kokius veiksmus atliko su savo atpažinties priemone – „Smart-ID" Paskyra Nr. 1 – analizuojamų aplinkybių metu. Pareiškėjas, pateikdamas papildomus paaiškinimus, nurodė, kad jungiantis prie suklastotos banko interneto banko svetainės jokių duomenų, išskyrus interneto banko naudotojo ID ir „Smart-ID" Paskyros Nr. 1 PIN1 kodą, nebuvo prašoma suvesti. Vis dėto banko kartu su atsiliepimu pateikti vidaus sistemų duomenys rodė, kad sutikimas sukurti „Smart-ID" Paskyrą Nr. 2 buvo duotas iš pareiškėjo įprastai naudojamo galinio įrenginio, suvedant pareiškėjo naudotos Paskyros Nr. 1 PIN2 kodą. Be to, banko pateiktais duomenimis, tretiesiems asmenims jungiantis prie banko interneto banko su „Smart-ID" Paskyra Nr. 2, buvo panaudotas ne tik pareiškėjo banko interneto banko naudotojo ID numeris, bet ir asmens kodas[6].

Įrodymų pakankamumas civiliniame procese grindžiamas tikėtinumo taisykle (tikimybių pusiausvyros principas). Kasacinio teismo jurisprudencijoje ne kartą pažymėta, kad įrodinėjimas civiliniame procese turi savo specifiką. Nenustatyta, kad išvadą apie tam tikrų faktų buvimą galima daryti tik tada, kai dėl jų egzistavimo absoliučiai nėra abejonių; išvadą apie faktų buvimą teismas civiliniame procese gali daryti ir tada, kai tam tikros abejonės dėl fakto buvimo išlieka, tačiau byloje esančių įrodymų visuma leidžia manyti esant labiau tikėtina atitinkamą faktą buvus, nei jo nebuvus[7]. Nors pareiškėjas teigia, kad suklastotoje interneto banko svetainėje suvedė tik savo interneto banko naudotojo ID, o vėliau, iššokus raginantiems tai padaryti „Smart-ID" Paskyros Nr. 1 pranešimams, suvedė šios paskyros PIN1 kodą, ginčo byloje turimais duomenimis, kuriant naują Smart-ID" paskyrą pareiškėjo vardu (t. y. Paskyrą Nr. 2), buvo panaudotas (taigi ir suvestas) ir „Smart-ID" Paskyros Nr. 1 PIN2 kodas. Nesant kitų galimybių nustatyti ir (ar) ginčo nagrinėjimo metu nenustačius kitokias aplinkybes pagrindžiančių duomenų (kaip „Smart-ID" Paskyra Nr. 2 galėjo būti sukurta pareiškėjui suvedus tik Paskyros Nr. 1 PIN1 kodą, o tretieji asmenys, jungdamiesi prie banko interneto banko aplinkos naudodamiesi Paskyra Nr. 2 iš savo galinio įrenginio, galėjo tai padaryti nepanaudodami pareiškėjo asmens kodo ar kaip pareiškėjo asmens kodą tretieji asmenys galėjo sužinoti kitais būdais, pačiam pareiškėjui suvedus tik naudotojo ID ir „Smart-ID" Paskyros Nr. 1 PIN1 kodą), neginčijant aplinkybės, kad Operacija yra neautorizuota ir jos įvykdyti savo valia pareiškėjas nesiekė, labiau tikėtina, kad būtent pareiškėjas atskleidė visus duomenis, būtinus prisijungti prie banko interneto banko, o „Smart-ID" Paskyros Nr. 2 sukūrimą patvirtino suvesdamas naudojamos „Smart-ID" Paskyros Nr. 1 PIN2 kodą.

Tobulėjant technologijoms, tobulėja sukčiavimo būdai ir priemonės, sudėtingesnės tampa sukčiavimo atakos, todėl jas atpažinti ir nuo jų apsisaugoti reikia vis didesnio mokėjimo paslaugų vartotojų atidumo ir rūpestingumo. Naujiems sukčiavimo būdams, panaudojant naujas technologijas, atpažinti būtina, kad vartotojai būtų itin pastabūs ir apdairūs. Tačiau kartais dėl sukčiavimo atakos naujumo ir kompleksiškumo vidutinio vartotojo gebėjimų gali

[6] Asmens kodą prašoma suvesti vartotojui jungiantis iš jam nebūdingo galinio įrenginio.
[7] Lietuvos Aukščiausiojo Teismo Civilinių bylų skyriaus teisėjų kolegijos 2008 m. rugpjūčio 25 d. nutartis civilinėje byloje Nr. 3K-3-304/2008; 2009 m. kovo 16 d. nutartis civilinėje byloje Nr. 3K-3-101/2009 ir kt.

nepakakti, kad būtų laiku identifikuotas mėginimas neteisėtu būdu pasisavinti mokėjimo priemonę ir (ar) įvykdyti mokėjimo operacijas, kurių mokėjimo paslaugų vartotojas nesiekia įvykdyti. Dėl to manytina, kad mokėjimo paslaugų teikėjai, kaip savo srities profesionalai, turi dėti reikiamas pastangas, kad nuolat kryptingai ir tinkamai informuotų savo klientus (vartotojus) apie sukčiavimo pavojus ir rizikas, susijusias su sukčiavimais elektroninėje erdvėje, ir primintų, kokie ir kaip vartotojų duomenys turėtų būti saugomi ir neatskleidžiami tretiesiems asmenims.

Bankas teigė, kad rūpindamasis klientų lėšų saugumu periodiškai juos informuoja ir teikia saugaus naudojimosi banko teikiamomis elektroninėmis paslaugomis rekomendacijas. Pavyzdžiui, 2020 m. balandžio 1 d. – 2020 m. balandžio 2 d. interneto banko žinute visiems klientams, tarp jų ir pareiškėjui, išsiuntė tokio turinio informaciją: „Svarbu! Susipažinkite su atnaujintomis saugumo rekomendacijomis. „<...> Būkite budrūs! Niekam neatskleiskite savo duomenų, jei patys neskambinate mums ar neatliekate operacijų. <...> Jei į Jus besikreipiantis asmuo žino Jūsų vardą, pavardę ar kitų asmeninio gyvenimo detalių, prisistato policijos pareigūnu, banko darbuotoju, investavimo specialistu ar pan., neprivalote jais besąlygiškai tikėti. Gavus SMS žinutę ar el. laišką su nuoroda, nebūtina jos spausti ir vykdyti pateiktų nurodymų. Be to, nuorodos gali vesti į suklastotus puslapius, panašius į bankų ar kitų organizacijų interneto svetaines.<...>". Šios rekomendacijos, banko teigimu, yra kas kartą matomos ir jungiantis prie interneto banko paslaugos. Bankas periodiškai perspėja klientus apie su sukčiavimu susijusias rizikas, išplatindamas pranešimus žiniasklaidai, o 2020 m. spalio 9 d. ir 2021 m. liepos 15 d. banko programėlės naudotojus pirmojo prisijungimo metu papildomai įspėjo tekstu, kurio negalima nepastebėti, o aplinkybę, kad šį tekstą perskaitė, papildomai reikėjo patvirtinti paspaudžiant mygtuką „OK".

Vertinant banko veiksmus, kurių jis ėmėsi, kad informuotų savo klientus, tarp jų ir pareiškėją, apie elektroninėje erdvėje kylančias rizikas naudojantis mokėjimo paslaugomis, pažymėtina, kad ginčo šalių sutartinių santykių neatskiriama dalimi esančiuose dokumentuose (banko ir pareiškėjo sudarytoje elektroninių paslaugų teikimo sutartyje ir mokėjimo paslaugų teikimo sąlygose) tapatybės patvirtinimo priemonės „Smart-ID" tiek PIN2 kodo, tiek apskritai PIN kodų suvedimas ir jų reikšmė mokėjimo operacijoms autorizuoti ar naudotis kitomis banko paslaugomis nėra atskirai detalizuojami. Taigi ginčo byloje nėra duomenų, kad pareiškėjas būtų tinkamai supažindintas su informacija, kokius veiksmus naudodamasis „Smart-ID" programėle jis gali atlikti, o kokie veiksmai ir kokiais atvejais (naudojantis šia tapatybės patvirtinimo priemone ir suvedant jos PIN kodus) sukelia atitinkamas teisines pasekmes sutartiniuose santykiuose su banku. Tokia informacija kiek plačiau atskleidžiama tik banko interneto svetainėje adresu https://www.swedbank.lt/static/pdf/private/home/more/Smart_ID_atmintine_2019-11.pdf.

Bankas, paaiškindamas pareiškėjo supažindinimo su programėlės „Smart-ID" naudojimosi ypatumais procesą, taip pat ir PIN kodų suvedimo reikšmę, nurodė, kad, prieš duodant sutikimą sukurti Paskyrą Nr. 2, pareiškėjui jo turimo įrenginio ekrane esančioje „Smart-ID" programėlės aplinkoje buvo rodomas tekstas, informuojantis apie veiksmą, kuriam pareiškėjas duoda sutikimą, t. y. kad kreipiamasi dėl naujos „Smart-ID" paskyros sukūrimo ir rodomas pasirinkimas „Patvirtinti" arba „Atšaukti". Atsiliepime nurodoma, kad pareiškėjas pasirinko „Patvirtinti", suvedė tik jam vienam žinomą Paskyrai Nr. 1 taikomą PIN2 kodą ir taip patvirtino sutikimą sukurti naują „Smart-ID" paskyrą (Paskyra Nr. 2) trečiųjų asmenų turimame įrenginyje. Taigi, nors šalių sutartinius santykius nustatantys dokumentai neapibrėžia pareiškėjo naudojamos tapatybės patvirtinimo priemonės „Smart-ID" ir jos PIN kodų suvedimo teisinės reikšmės pareiškėjo santykiuose su banku, nagrinėjamu atveju bankas pateikė duomenis, kad, prieš pareiškėjui duodant sutikimą sukurti savo vardu naują „Smart-ID" Paskyrą Nr. 2, jo valdomame įrenginyje esančios „Smart-ID" programėlės Paskyroje Nr. 1 buvo rodomi pranešimai, aiškiai ir nedviprasmiškai detalizuojantys, kokiam veiksmui patvirtinti buvo prašoma suvesti Paskyros Nr. 1 PIN1 ir PIN2 kodus. Be to, naudodamiesi mokėjimo paslaugomis elektroninėje erdvėje vartotojai privalo paisyti saugaus elgesio rekomendacijų ir, pagrįstai tikėdamiesi aukštus profesionalumo, rūpestingumo ir atidumo standartus atitinkančio mokėjimo paslaugų teikėjo elgesio, patys būti apdairūs, atidūs ir sąmoningi, nes vartotojų lėšų ir atliekamų mokėjimo operacijų, kaip ir kitų elektroninėje erdvėje teikiamų mokėjimo paslaugų, saugumas priklauso ir nuo tinkamo bei atidaus mokėjimo paslaugų vartotojų pareigų, susijusių su mokėjimo priemonių naudojimu, vykdymo.

Kaip minėta, Mokėjimų įstatymo 34 straipsnyje nustatyta viena iš mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigų – naudotis mokėjimo priemone

pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas. Banko mokėjimo paslaugų teikimo sąlygų 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 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)".

Be to, banko viešai skelbiamose saugaus naudojimosi elektroninėmis paslaugomis rekomendacijose banko klientai raginami nespausti jokių elektroniniu 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[8].

Iš banko mokėjimo paslaugų teikimo sąlygų nuostatų matyti, kad jose aiškiai ir nedviprasmiškai reglamentuojama, kad už tapatybės priemonės personalizuotų saugumo duomenų konfidencialumą yra atsakingas mokėtojas, šiuo atveju – pareiškėjas. Atsižvelgiant į tai, manytina, jog pareiškėjo elgesys būtų laikomas atitinkančiu mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, jei būtų nustatyta, kad jis ėmėsi adekvačių veiksmų (arba nuo tam tikrų veiksmų susilaikė), kad būtų tinkamai užtikrintas banko išduotų mokėjimo priemonių personalizuotų saugumo duomenų, sudarančių sąlygas inicijuoti ir tvirtinti mokėjimus, konfidencialumas.

Įvertinus ginčo bylos duomenis ir kitas nustatytas aplinkybes, vis dėlto negalima daryti išvados, kad pareiškėjo elgesys atitiko banko nustatytas naudojimosi mokėjimo priemonėmis sąlygas ir buvo adekvatus bei pakankamas, kad pareiškėjui nustatytos pareigos, susijusios su mokėjimo priemonių personalizuotų saugumo duomenų konfidencialumo užtikrinimu, būtų tinkamai įvykdytos. Nors pareiškėjui į mobilųjį telefoną atsiųsta SMS žinutė galėjo sukurti pirminį įspūdį, kad išsiųsta iš banko, tačiau tai, kad pareiškėjas iki personalizuotų duomenų atskleidimo (pateikimo suklastotoje interneto svetainėje) nesudvejojo nurodytos informacijos ir pagal pateiktą nuorodą atsidariusio interneto puslapio patikimumu, taip pat nekvestionuodamas pateiktų nurodymų pagrįstumo suvedė, kaip nustatyta ginčo nagrinėjimo metu, savo interneto banko naudotojo ID ir asmens kodą, o vėliau ir naudojamos „Smart-ID" Paskyros Nr. 1 PIN1 ir PIN2 slaptažodžius, atsiradus tai padaryti raginantiems „Smart-ID" programėlės pranešimams, leidžia teigti, kad pareiškėjo elgesys aptariamų aplinkybių metu nebuvo itin apdairus ir atsargus.

Sprendžiant dėl pareiškėjo neatsargumo laipsnio, būtina atkreipti dėmesį į tai, kad trečiųjų asmenų pareiškėjui siųsta SMS žinutė, parašyta be lietuviškų rašmenų, informavo pareiškėją apie tai, kad jo „SmartID" paskyra „uzblokuota del saugumo" ir tam, kad pareiškėjas užkirstų kelią tariamam „Smart-ID" programėlės užblokavimui, jis turi spausti pateiktą nuorodą. Pareiškėjas nurodė, kad, paspaudus nuorodą sukčių siųstame SMS pranešime, matėsi standartinis banko prisijungimo prie elektroninės bankininkystės puslapis, per kurį pareiškėjas teigia bandęs prisijungti prie savo interneto banko, suvesdamas PIN1 kodą, tačiau prisijungti nepavyko. Vis dėlto aplinkybė, kad pagal SMS pranešimo nurodymus nepavyko užkirsti kelio tariamam „Smart-ID" programėlės užblokavimui, pareiškėjui nesukėlė abejonių ar poreikio atlikti papildomus veiksmus. Pagal nustatytas aplinkybes ir ginčo byloje turimus duomenis, pareiškėjas negalėjo prisijungti prie savo interneto banko, kad galėtų atlikti SMS pranešime nurodytus veiksmus (užkirstų kelią „Smart-ID" programėlės užblokavimui), tačiau į banką

[8] https://www.swedbank.lt/static/pdf/legalisation/private/mokejimu_paslaugu_teikimo_salygos_2019-12-09.pdf.

paskambino tik elektroniniu paštu gavęs pranešimą, kad jo vardu sukurta nauja „Smart-ID" paskyra.

Aptariamų aplinkybių kontekste įvertintina ir trečiųjų asmenų siųstoje SMS žinutėje pateikta nuoroda HK38721.com. Nagrinėdamas dėl neautorizuotų mokėjimo operacijų, atliktų įvykus sukčiavimo atakai, kilusius ginčus Lietuvos bankas yra pažymėjęs, kad vien tik faktas, jog vartotojas paspaudė jam SMS žinute atsiųstą aktyvią nuorodą ir nepastebėjo, kad pateko ne į tikrą banko interneto puslapį, o į trečiųjų asmenų suklastotą banko interneto puslapį, savaime nereiškia vartotojo didelio neatsargumo. Tačiau nagrinėjamu atveju būtina atkreipti dėmesį į tai, kad trečiųjų asmenų pareiškėjui atsiųstoje SMS žinutėje pateikta aktyvi nuoroda buvo visiškai nepanaši į tikrąją banko interneto banko nuorodą – jos pavadinime nebuvo jokio panašumo į jungiantis prie banko interneto banko matomą informaciją (pvz., nurodytas klaidingas banko pavadinimas vizualiai galėtų atrodyti panašus į tikrąjį banko pavadinimą ir pan.). Be to, kaip atsiliepime pažymėjo bankas, SMS pranešimo tekste „Smart-ID" pavadinimas įrašytas su klaida, o pats telefono numeris, iš kurio siųstas aptariamas SMS pranešimas, yra ne su Lietuvos kodu + 370. Manytina, kad šios aplinkybės, kurios vidutiniškai apdairų ir rūpestingą vartotoją būtų privertusios rimtai sudvejoti atliekamų veiksmų ir pateiktų prašymų pagrįstumu, pareiškėjui galėjo nesukelti jokių abejonių tik dėl to, kad jis buvo itin neatidus.

Sprendžiant dėl pareiškėjo neatsargumo laipsnio, teisiškai reikšminga ir viena iš jo elgesio vertinimą lemiančių aplinkybių, kad, ginčo byloje esančiais duomenis[9], pareiškėjas, prieš suvesdamas Paskyros Nr. 1 PIN2 slaptažodį, ne tik gavo ir matė pranešimą, raginantį įsitikinti, kad atliekamos operacijos (veiksmo) informacija yra teisinga, bet ir informuojantį, jog šia operacija siekiama sukurti naują „Smart-ID" paskyrą. Šiuose jo telefone pasirodžiusiuose programėlės „Smart-ID" pranešimuose reikėjo paspausti „Patvirtinti" ir tik tada suvesti prašomą Paskyros Nr. 1 PIN2 slaptažodį. Bankas, remdamasis vidaus sistemos duomenimis, nurodė, kad, prieš pareiškėjui duodant sutikimą sukurti Paskyrą Nr. 2, jo turimo įrenginio ekrane esančioje „Smart-ID" programėlės aplinkoje buvo rodomas tekstas, informuojantis apie veiksmą, kuriam duodamas sutikimas: „Patvirtinkite informaciją. Norėdami tęsti, įsitikinkite, kad Jūsų operacijos informacija yra teisinga: „Applying for new Smart-ID account", ir rodomas pasirinkimas „Patvirtinti" arba „Atšaukti". Pareiškėjas turėjo pasirinkti „Patvirtinti" ir suvesti tik jam vienam žinomą Paskyrai Nr. 1 taikomą PIN2 (taip buvo patvirtintas sutikimas naujai „Smart-ID" paskyrai pareiškėjo vardu (Paskyrai Nr. 2) trečiųjų asmenų turimame įrenginyje sukurti).

Aplinkybė, kad pareiškėjas neužtikrino savo personalizuotų saugumo duomenų konfidencialumo ir suvedė „Smart-ID" paskyros PIN2 kodą, faktiškai (kaip patvirtina ginčo byloje esantys įrodymai) turėdamas matyti, kam išreiškia sutikimą, lėmė, kad pareiškėjo vardu buvo ne tik sukurta nauja tapatybės patvirtinimo priemonės „Smart-ID" paskyra trečiųjų asmenų kontroliuojamame mobiliajame įrenginyje, bet ir iš jo banko Sąskaitos įvykdyta jo neautorizuota Operacija, kurią atliekant pareiškėjas nedalyvavo, savo sutikimo nedavė ir net nežinojo apie Operacijos inicijavimą ir patvirtinimą.

Ginčo byloje esantys įrodymai ir ginčo nagrinėjimo metu nustatytos aplinkybės, susijusios su sukčiavimo atakos pobūdžiu, banko, o svarbiausia – paties pareiškėjo veiksmais, vis dėlto nesudaro pagrindo pareiškėjo elgesį laikyti tik neatsargiu, net įvertinus tai, kad sukčiavimo ataka buvo sofistikuota ir ją pastebėti buvo būtinas pareiškėjo atidumas ir rūpestingumas, nes pareiškėjui siųstuose pranešimuose, prašant suvesti Paskyros Nr. 1 PIN2 kodą, buvo rodoma tiksli ir teisinga informacija, dėl kokio veiksmo jis išreiškia sutikimą suvesdamas PIN2 kodą. Tai, kad pareiškėjo elgesys sudarant sąlygas tretiesiems asmenims užvaldyti jo Sąskaitą buvo labai neatsargus, sustiprina ir aplinkybė, kad pareiškėjas nesudvejojo trečiųjų asmenų atsiųstame SMS pranešime be lietuviškų rašmenų nurodytos informacijos patikimumu ir nekvestionuodamas paspaudus nuorodą atsidariusio interneto puslapio autentiškumo suvedė savo naudotojo ID ir asmens kodą, taip atskleisdamas tretiesiems asmenims savo personalizuotus saugumo duomenis ir sudarydamas sąlygas inicijuoti naujos „Smart-ID" paskyros sukūrimą.

Lietuvos banko vertinimu, aptartos aplinkybės leidžia teigti, kad pareiškėjas, nesilaikydamas jam kaip mokėjimo paslaugų vartotojui nustatytų pareigų, susijusių su

[9] Bankas kartu su papildomais paaiškinimais pateikė vidaus sistemų duomenis, kokio turinio standartiniai pranešimai klientams, besinaudojantiems „Smart-ID" kaip tapatybės patvirtinimo priemone, buvo siunčiami tuo laikotarpiu, kai buvo įvykdyta Operacija, ir įrodymus, kad, prieš pareiškėjui suvedant „Smart-ID" Paskyros Nr. 1 PIN2 kodą, jam buvo išsiųstas ir rodomas pranešimas, informuojantis, kad suvesdamas šios paskyros PIN2 kodą, jis tvirtina naujos „Smart-ID" paskyros sukūrimą: *Applying for new Smart-ID account* (liet. kreipiamasi dėl naujos „Smart-ID" paskyros).

mokėjimo priemonės naudojimu, nebuvo tiek atidus ir rūpestingas, kiek akivaizdžiai buvo būtina nurodytomis aplinkybėmis. Jei pareiškėjas būtų laikęsis bent minimalių atsargumo ir dėmesingumo reikalavimų, jis būtų ne tik sudvejojęs iš nepažįstamo siuntėjo gautos SMS žinutės, parašytos nelietuviškai rašmenimis ir išsiųstos iš užsienietiško telefono numerio, turinio ir pateiktos nuorodos, neturinčios jokio panašumo nei į banko, nei į „Smart-ID" kūrėjų interneto svetainės adresą, patikimumu, bet ir būtų perskaitęs „Smart-ID" gautuose pranešimuose nurodytą tekstą, kad būtina įvertinti, kokiam veiksmui duoda sutikimą suvesdamas PIN2 kodą. Toks pareiškėjo elgesys lėmė, kad tretieji asmenys įgijo galimybę sukurti naują „Smart-ID" paskyrą pareiškėjo vardu trečiųjų asmenų kontroliuojamame mobiliajame įrenginyje ir iš ten patvirtinti jų inicijuotą Operaciją. Tai suponuoja išvadą, kad pareiškėjo elgesys (būtinų saugumo rekomendacijų ir jam kaip mokėjimo paslaugų vartotojui nustatytų pareigų nesilaikymas, galiausiai lėmęs ir Operacijos įvykdymą bei jos sumos nurašymą iš pareiškėjo Sąskaitos banke) gali būti vertinamas kaip didelis neatsargumas (aplaidumas), todėl visi nuostoliai, susiję su šios Operacijos įvykdymu, turėtų tekti pareiškėjui.

Konstatavus, kad pareiškėjas, nesilaikydamas jam kaip mokėtojui Mokėjimų įstatyme ir sutartyje su banku nustatytų pareigų, susijusių su išduotomis mokėjimo priemonėmis, elgėsi labai neatsargiai, 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 to, Lietuvos banko vertinimu, bankas neprivalo grąžinti (kompensuoti) pareiškėjui neautorizuotos Operacijos lėšų.

Dėl banko pareigos grąžinti mokėjimo operacijos, įvykdytos po to, kai mokėtojas praneša apie mokėjimo priemonės praradimą ir neautorizuotą jos panaudojimą, lėšas

Pareiškėjas kreipimesi teigė, kad po pirmojo pokalbio su banko darbuotoja jo vardu sukurta Paskyra Nr. 2 nebuvo užblokuota (nors elektroniniu laišku buvo pranešta, kad užblokuota). Pareiškėjo teigimu, tai sudarė palankias sąlygas tretiesiems asmenims atlikti veiksmus jo Sąskaitoje, t. y. inicijuoti ir patvirtinti Operaciją.

Pagal Mokėjimų įstatymo 34 straipsnio 1 dalies 2 punktą, mokėtojas, sužinojęs apie mokėjimo priemonės praradimą, vagystę arba neteisėtą pasisavinimą ar neautorizuotą jos naudojimą, nedelsdamas apie tai turi pranešti mokėjimo paslaugų teikėjui arba jo nurodytam subjektui. Pagal Mokėjimų įstatymo 39 straipsnio 5 dalį, mokėtojas neturi patirti jokių nuostolių dėl prarastos, pavogtos ar neteisėtai pasisavintos mokėjimo priemonės po to, kai pateikia šio įstatymo 34 straipsnio 1 dalies 2 punkte nurodytą pranešimą, išskyrus atvejus, kai jis veikė nesąžiningai.

Ginčo byloje nustatytais duomenimis, 2021 m. rugsėjo 1 d. 19:10 val. pareiškėjas skambino „Smart-ID" kūrėjams telefonu + 370 670 41 807, o į banką, siekdamas informuoti apie gautas SMS žinutes ir galbūt įvykusį sukčiavimo atvejį, paskambino tik 19:48 val. ir 20:13 val. Antrojo pokalbio su pareiškėju metu banko darbuotoja, gavusi pareiškėjo pranešimą apie Operaciją, 20:32:47 val. blokavo pareiškėjui prisijungti prie interneto banko išduotą naudotojo numerį (taip buvo užblokuota pareiškėjui teikiama interneto banko paslauga), iš „Smart-ID" duomenų bazės per banko informacinę sistemą 20:29:49 val. pašalino (ištrynė) Paskyrą Nr. 2, o 20:29:49 val. – Paskyrą Nr. 1. Nustatyta, kad Operacija buvo įvykdyta 19:09:19 val., taigi dar iki pirmojo pareiškėjo skambučio į banką, taip pat ir iki (ginčo byloje esančiais duomenimis) pareiškėjo bandymo susisiekti su „Smart-ID" kūrėjais.

Bankas, atsiliepime paaiškindamas Paskyros Nr. 1 pašalinimo ir bandymo atšaukti pareiškėjo vardu pateiktą mokėjimo nurodymą įvykdyti Operaciją aplinkybes, nurodė, kad pareiškėjo ir banko darbuotojo pirmojo telefoninio pokalbio metu, banko darbuotojui siekiant nustatyti pareiškėjo tapatybę, į pareiškėjo įrenginį buvo siunčiama „Smart-ID" užklausa, kurią pareiškėjas turėjo patvirtinti į automatiškai telefono ekrane atsidariusį „Smart-ID" programėlės langą suvesdamas Paskyros Nr. 1 PIN1 slaptažodį. Banko teigimu, tikėtina, kad dėl tuo pačiu metu vykdomo pokalbio su banko darbuotoju pareiškėjui nepavyko atlikti šio veiksmo, todėl banko darbuotoja paprašė pareiškėjo perskambinti iš kito įrenginio, kad būtų galima tinkamai nustatyti pareiškėjo tapatybę prieš atliekant mokėjimo priemonių blokavimo veiksmus. Antrojo pokalbio metu pareiškėjas nurodė, kad elektroniniu paštu gavo laišką apie jo vardu sukurtą „Smart-ID" paskyrą, kuriame buvo raginama susisiekti nurodytu telefonu tuo atveju, jei paskyrą sukūrė ne pareiškėjas. Pareiškėjas paaiškino, kad susisiekus nurodytu telefonu atsiliepęs asmuo prisistatė banko darbuotoju ir paklausė pareiškėjo asmens kodo ir telefono modelio, o kai pareiškėjas patikslino šią informaciją, elektroniniu paštu gavo pranešimą, informuojantį apie nereikalingos paskyros panaikinimą. Pokalbio su banko darbuotoja metu

pareiškėjas negalėjo nurodyti telefono numerio, į kurį skambino, tačiau pažymėjo, kad jis skyrėsi nuo banko oficialaus telefono numerio, o skambinimo laiką pareiškėjas įvardijo kaip „apytiksliai be dvidešimt minučių septintą valandą". Banko manymu, labiausiai tikėtina, kad pareiškėjas tuo metu supainiojo „Smart-ID" kūrėjus su banku ir turėjo omenyje 2021 m. rugsėjo 1 d. 19:10 val. skambutį „Smart-ID" kūrėjams. Pažymėtina, kad ginčo byloje nėra duomenų, jog, be nurodytų bandymų, pareiškėjas būtų bandęs papildomai susisiekti su banku ar „Smart-ID" kūrėjais, kad informuotų apie galimą mokėjimo priemonės praradimą.

Nurodytos aplinkybės leidžia teigti, kad pareiškėjas apie mokėjimo priemonės (prieigos prie interneto banko) praradimą informavo banką jau po ginčijamos Operacijos inicijavimo ir patvirtinimo. Be to, jau pirmojo pareiškėjo skambučio metu bankas ne tik neturėjo pareigos atšaukti mokėjimo nurodymą įvykdyti Operaciją, nes jau buvo praėjęs Mokėjimų įstatyme nustatytas momentas, iki kurio galima atšaukti mokėjimo nurodymą[10], bet net ir neturėjo galimybės tai padaryti. Nustatyta, kad Operacija įvykdyta kaip momentinis mokėjimas (per kelias ar keliolika sekundžių), todėl bankas, kai paskambino pareiškėjas, neturėjo galimybės jos atšaukti, nes ji jau buvo įvykdyta.

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

[10] Mokėjimų įstatymo 44 straipsnio 1 dalis nustato, kad mokėjimo paslaugų vartotojas negali atšaukti mokėjimo nurodymo po to, kai jį gauna mokėtojo mokėjimo paslaugų teikėjas, išskyrus šiame straipsnyje nustatytas išimtis. Šio straipsnio 4 dalis nustato, 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.