LIETUVOS BANKO
TEISĖS IR LICENCIJAVIMO DEPARTAMENTO
DIREKTORIUS

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

2022 m. birželio 16 d. Nr. 429-240
Vilnius

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

N u s t a t y t a:

Ginčo nagrinėjimo metu nustatytais duomenimis, 2021 m. spalio 21 d. 18:52 val. pareiškėja į savo mobilųjį telefoną gavo trečiųjų asmenų siųstą SMS pranešimą, kuriuo buvo įspėta dėl interneto banko sutarties blokavimo ir paraginta spausti tame pačiame SMS pranešime pateiktą nuorodą: „Jūsų interneto banko sutartis užblokuota apsilankykite seb.login20.com.“

Gavusi SMS pranešimą, pareiškėja paspaudė jame pateiktą nuorodą *seb.login20.com* ir atsidariusiame trečiųjų asmenų sukurtame interneto tinklalapyje suvedė savo interneto banko atpažinimo kodą (ID), asmens kodą ir savo mobiliajame įrenginyje į savo naudojamą „Smart-ID“ paskyrą (toliau - Paskyra1), gavusi patvirtinimo užklausas, suvedė „Smart-ID“ Paskyros1 PIN1 ir PIN2 kodus.

2021 m. spalio 21 d. 18:54 val. tretieji asmenys savo įrenginyje pareiškėjos vardu sukūrė „Smart-ID Basic“ paskyrą (toliau – Paskyra2).

2021 m. spalio 21 d. 19:07 val. tretieji asmenys, naudodamiesi Paskyra2, pareiškėjos vardu aktyvavo *SEB* mobiliąją programėlę trečiųjų asmenų valdomame mobiliajame įrenginyje ir prie jos prisijungę atliko mokėjimus iš trijų skirtingų pareiškėjos sąskaitų banke: 1) 2021 m. spalio 21 d. nuo 19:07 iki 19:57 val. – bendra suma 19 630 eurų (iš sąskaitos Nr. (*duomenys neskelbtini*)); 2) 2021 m. spalio 21 d. nuo 19:08 val. iki 19:22 val. – bendra suma 2 900 eurų (iš sąskaitos Nr. (*duomenys neskelbtini*)); 3) 2021 m. spalio 21 d. nuo 19:52 val. iki 20:05 val. – bendra suma 47 717 eurų (iš sąskaitos Nr. (*duomenys neskelbtini*)) (toliau – Ginčijami mokėjimai). Tretieji asmenys taip pat atliko vidinius mokėjimus ir tarp pareiškėjos sąskaitų banke: 1) 2021 m. spalio 21 d. iš sąskaitos Nr. (*duomenys neskelbtini*) į sąskaitą Nr. (*duomenys neskelbtini*), 12 000 Eur (19:23 val.); 2) 2021 m. spalio 21 d. iš sąskaitos Nr. (*duomenys neskelbtini*) į sąskaitą Nr. (*duomenys neskelbtini*), 6 000 Eur (19:38 val.); 3) 2021 m. spalio 21 d. iš sąskaitos Nr. (*duomenys neskelbtini*) į sąskaitą Nr. (*duomenys neskelbtini*), 10 000 Eur (19:52 val.). Dalies Ginčijamų mokėjimų, kurių bendra suma sudaro 12 497,91 euro, lėšų gavėjo mokėjimo paslaugų teikėjas neįskaitė į lėšų gavėjo sąskaitą (-as) ir jas grąžino atgal į pareiškėjos sąskaitas.

2021 m. spalio 21 d. 20:10 val. pareiškėja telefonu kreipėsi į banką ir pranešė apie sukčiavimo atvejį. Bankas po pareiškėjos skambučio užblokavo jos interneto banko paskyrą ir prieigą prie SEB mobiliosios programėlės, dėl pareiškėjos vardu naujai sukurtos „Smart-ID Basic“ paskyros Paskyra2 atšaukimo rekomendavo kreiptis į „Smart-ID“ leidėjos *SK ID solutions AS* (toliau – SK) Lietuvos filialą, taip pat rekomendavo pareiškėjai dėl sukčiavimo kreiptis į teisėsaugos institucijas.

2021 m. spalio 22 d. bankas kreipėsi į lėšų gavėjų mokėjimo paslaugų teikėjus *Revolut LTD* ir *N26 Bank* dėl Ginčijamų mokėjimų lėšų grąžinimo.

2021 m. spalio 26 d. ir 2021 m. lapkričio 3 d. bankas gavo atsakymus iš lėšų gavėjų mokėjimo paslaugų teikėjų, kad nėra galimybės susigrąžinti Ginčijamų mokėjimų, kurie buvo įvykdyti kaip momentiniai mokėjimai, lėšų, ir apie tai informavo pareiškėją žinute interneto banke.

Pareiškėja nesutinka su banko sprendimu nekompensuoti jos nuostolių, susijusių su

Ginčijamų mokėjimų įvykdymu. Paaiškindama aplinkybes, susijusias su sukčiavimo ataka, lėmusia Ginčijamų mokėjimų įvykdymą, pareiškėja kreipimesi nurodo, kad 2021 spalio 21 d. pirmoje dienos pusėje atliko kelis mokėjimus, naudodamasi banko interneto banku. Pareiškėjos teigimu, mokėjimus pavyko atlikti, nors „Smart-ID" programėlė „striginėjo", o po to buvo lyg „pakibusi", tačiau ją pavyko uždaryti. Toliau kreipimesi nurodoma, kad pareiškėjai „po sunkios darbo dienos, pavargusiai, vakare 18.52 atėjo pranešimas, iš SEB banko, kad Jūsų banko sutartis užblokuota apsilankykite seb.login20.com. Kadangi dienos metu turėjau problemų, kilo mintis, kas čia dar nutiko ir automatiškai ją atidariau, išsigandusi, kodėl ji užblokuota. Atsidariau Smart ID, suvesdama, ką įprastai darydavau. Atsidaryti, programiniai laukai, nesukėlė jokio įtarimo. Trumpinio nuoroda „.com" irgi pasirodė įtikinanti. Sau, patvirtinau, kad su paskyra viskas gerai, ir pamaniau, kad vėl klaidžioja kažkokios programinės klaidos. Antroji žinutė kad registruojama paskyra, kurios nepamačiau, įkrito, man atsidarius nurodytą tinklapį, kas ir buvo lemtinga." Pareiškėja teigia, kad vėliau vakare (20:01 val.) gavo SMS pranešimą iš banko, kad vyksta sukčiavimo ataka ir banko klientai turėtų nespausti pranešimuose banko vardu pateiktų nuorodų ir neatskleisti savo mokėjimo priemonių duomenų. Paskambinusi į banką, pareiškėja sužinojo, kad dėl trečiųjų asmenų įvykdytos sukčiavimo atako neteko sąskaitose banke buvusių lėšų – beveik 50 000 Eur. Pareiškėja teigia nesuprantanti, kodėl banko SMS žinutė, įspėjanti apie vykstančią sukčiavimo ataką, buvo išsiųsta pareiškėjai tik 20:01 val., nes sukčių banko vardu siųstus pranešimus ji gavo apie 19 val., tad jei pareiškėja, jos teigimu, įspėjantį banko pranešimą būtų gavusi anksčiau, ji nebūtų tapusi sukčių auka ir praradusi visų savo gyvenimo santaupų. Pareiškėja mano, kad lėšos banko sąskaitose nebuvo tinkamai apsaugotos – pareiškėjai nesuprantama, kodėl kuriant naują „Smart-ID" paskyrą jos vardu, nebuvo prašoma pateikti jos asmens kodo. Kreipimesi taip pat pažymima, kad trečiųjų asmenų siųsta žinutė pakliuvo į bendrą kitų banko siųstų žinučių srautą ir tai sumažino pareiškėjos budrumą, ypač dėl to, kad dienos metu „Smart-ID" programėlė neveikė sklandžiai, tad žinutės turinys pareiškėjai nepasirodė įtartinas. Pareiškėja mano, kad bankas turi įdiegti priemones, kad apsaugotų savo klientus ir jų sąskaitose esančias lėšas. Kreipimesi pareiškėja prašo rekomenduoti bankui kompensuoti pareiškėjai jos nuostolius dėl sukčių naudai įvykdytų Ginčijamų mokėjimų, kuriuos ji vertina 32 336 Eur suma[1].

Bankas nesutinka tenkinti pareiškėjos reikalavimo. Bankas mano, kad pareiškėja elgėsi neapdairiai ir itin neatsargiai, t. y. nesilaikė atidumo ir rūpestingumo reikalavimų: paspaudė neaiškią nuorodą, suvedė savo interneto banko ID, asmens kodą ir savo mobiliajame įrenginyje savo atliekamus veiksmus patvirtino suvesdama tik pareiškėjai žinomus Paskyros1 PIN1 ir PIN2 kodus, dėl to tretieji asmenys pareiškėjos vardu galėjo susikurti Paskyrą2, kurioje pareiškėjos vardu vėliau patvirtino Ginčijamus mokėjimus SEB mobiliojoje programėlėje. Atsiliepime nurodoma, kad pareiškėja ne tik nesilaikė jai su išduotomis mokėjimo priemonėmis susijusių pareigų, nustatytų teisės aktuose, šalių sutartinius santykius reglamentuojančiuose dokumentuose, bet ir SK nustatytų „Smart-ID" naudojimo reikalavimų – „Q Smart-ID" sertifikatų naudojimo nuostatų ir sąlygų" (toliau – Sąlygos), kuriose nustatyta „Smart-ID" vartotojo pareiga privatųjį raktą naudoti ir valdyti tik pačiam „Smart-ID" vartotojui, ir tai lėmė, kad tretieji asmenys pasisavino pareiškėjos tapatybę. Bankas pažymi, kad pareiškėja nereagavo į banko siųstą SMS pranešimą, kuriuo buvo informuota apie pareiškėjos vardu kuriamą Paskyrą2, bei raginimą nedelsiant kreiptis į banką, jeigu paskyrą kuria ne pareiškėja („Antroji žinutė kad registruojama paskyra, kurios nepamačiau, įkrito, man atsidarius nurodytą tinklapį, kas ir buvo lemtinga"). Pareiškėjos didelį neatsargumą, banko teigimu, rodo ir tai, kad pareiškėja nedvejodama suvedė tik jai žinomus Paskyros1 PIN1 ir PIN2 kodus trečiųjų asmenų sukurtoje interneto svetainėje, į kurią pareiškėja pateko paspaudusi SMS pranešime pateiktą nuorodą, kuri neatitinka banko interneto banko svetainės adreso, be to, pareiškėja neįsitikino nei pateiktos nuorodos, nei atsidariusio interneto puslapio patikimumu, nebandė kreiptis į banką ar „Smart-ID" leidėją SK, kad išsklaidytų abejones ar patikrintų gautų pranešimų ir (ar) interneto puslapio patikimumą, nes tokia informacija pareiškėjai turėjo kelti pagrįstų įtarimų.

Atsižvelgdamas į pareiškėjos teiginius dėl „Smart-ID" Paskyros2 sukūrimo, bankas paaiškino, kad kai pareiškėja pateko į sukčių ataką, ji naudojosi „Smart-ID" visateisės prieigos paskyra (Paskyra1). Gavusi sukčių siųstą SMS žinutę, paspaudusi nuorodą, suvedusi interneto banko prisijungimo duomenis (atpažinimo kodą ir asmens kodą) bei savo mobiliajame įrenginyje veiksmus patvirtinusi suvesdama tik jai žinomus „Smart-ID" PIN1 ir PIN2 kodus, pareiškėja sukčiams suteikė galimybę jų telefone įdiegti „Smart-ID Basic" paskyrą (Paskyrą2),

[1] Kaip minėta, dalies Ginčijamų mokėjimų lėšų gavėjo mokėjimo paslaugų teikėjas neįskaitė į lėšų gavėjo sąskaitą (-as) ir jas grąžino atgal į pareiškėjos sąskaitas.

kuriai sukurti nėra būtinas papildomas autentifikavimas papildomomis priemonėmis (t. y. registruojant paskyrą ir nustatant tapatybę užtenka naudoti interneto banką), ir kartu suteikė galimybę sukčiams pareiškėjos vardu aktyvuoti SEB programėlę ir joje atlikti mokėjimų nurodymus, tvirtinant juos naudojantis Paskyra2.

Bankas atsiliepime patvirtino, kad Ginčijamų mokėjimų inicijavimo ir patvirtinimo metu banko sistemos veikė saugiai, jokių sutrikimų užfiksuota nebuvo, ir teigė, kad deda pastangas ir vykdo visus reikalavimus, kad užtikrintų klientų lėšų saugumą, tačiau neturi galimybės kontroliuoti klientų neatsargių veiksmų, kurie nėra ir negali būti kontroliuojami banko ir siejami su juo. Bankas paaiškino, kad apie sukčių atakas sužino tik iš klientų kreipimųsi, t. y. klientams informavus banką apie gautas neaiškias SMS žinutes, ir tuomet nedelsdamas apie tai informuoja klientus tiek viešojoje erdvėje, tiek asmeniniais pranešimais, tačiau, banko teigimu, informacijos pateikimas klientams skirtingais kanalais reikalauja skirtingų banko veiksmų, kurių atlikimas užtrunka tam tikrą laikotarpį. Nagrinėjamu atveju bankas, gavę informaciją iš klientų apie vykstančią sukčių ataką, nedelsdamas paskelbė apie tai informaciją banko interneto puslapyje, papildomai klientus informavo ir SMS žinutėmis, kurių tekstas buvo toks: „Būkite budrūs: vyksta SMS sukčių ataka. Nespauskite gautų nuorodų ir neatskleiskite savo duomenų. SEB.“ Banko teigimu, dėl sudėtingesnio klientų informavimo tam tikrais Banko naudojamais kanalais SMS pranešimai klientus pasiekė skirtingu laiku. Įvertinęs aplinkybių visumą ir teisinį reglamentavimą, bankas mano, kad neturi pareigos pareiškėjai kompensuoti nuostolių, patirtų dėl Ginčijamų mokėjimų.

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 42^1 straipsnyje reglamentuojamų patikrinimų, skirtų faktinėms aplinkybėms dėl Lietuvos banko priežiūrimo 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 grąžinti ir (ar) kompensuoti pareiškėjai Ginčijamų mokėjimų, įvykdytų pareiškėjos vardu tretiesiems asmenims sukūrus naują tapatybės patvirtinimo priemonės „Smart-ID“ paskyrą jų kontroliuojamame įrenginyje, sumų. Pareiškėja mano, kad bankas nesiėmė tinkamų veiksmų, kad būtų užtikrintas jos banko sąskaitos ir joje esančių lėšų saugumas, todėl bankas yra atsakingas už pareiškėjos nuostolius, įvykdžius Ginčijamus mokėjimus sukčių naudai. Bankas teigia, kad tretieji asmenys įgijo sąlygas inicijuoti ir patvirtinti Ginčijamus mokėjimus tik dėl to, kad pareiškėja dėl didelio neatsargumo atskleidė savo mokėjimo priemonių personalizuotus saugumo duomenis tretiesiems asmenims ir naujos „Smart-ID“ paskyros (Paskyros2) sukūrimą patvirtino suvesdama savo naudojamos „Smart-ID“ paskyros (Pskyros1) PIN kodus, todėl Ginčijamų mokėjimų lėšų grąžinti ir (ar) kompensuoti pareiškėjai bankas neturi.

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, Ginčijami mokėjimai buvo inicijuoti ir įvykdyti trečiųjų asmenų, jiems neteisėtu būdu sužinojus (pasisavinus) pareiškėjos mokėjimo priemonių personalizuotus saugumo duomenis ir juos panaudojus naujai „Smart-ID“ paskyrai (Paskyrai2) pareiškėjos vardu sukurti, o vėliau ir patiems Ginčijamiems mokėjimams inicijuoti ir įvykdyti. Akivaizdu, kad Ginčijamų mokėjimų inicijavimas ir patvirtinimas neatitiko pačios pareiškėjos valios, nors formaliai (pagal išorinius požymius) ir sutapo su pareiškėjos ir banko sutarta

sutikimo atlikti mokėjimo operacijas davimo forma ir tvarka. Pareiškėjos nurodytos aplinkybės, kad Ginčijami mokėjimai nėra pareiškėjos autorizuoti, bankas atsiliepime neginčija, todėl šio ginčo nagrinėjimo metu Lietuvos bankas daro išvadą, kad Ginčijami mokėjimai, atlikti nesant pareiškėjos valios ir jai net nežinant apie Ginčijamų mokėjimų inicijavimo aplinkybę bei neišreiškus jokių valinių veiksmų, kad Ginčijami mokėjimai būtų patvirtinti, laikytini neautorizuotais.

Dėl neautorizuotų mokėjimo operacijų pasekmių ir pareiškėjos teisės į Ginčijamų mokėjimų 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 dalyje nustatyta, 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 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 įstatyme aiškiai nustatyta, 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 pareiškėja galėjo veikti nesąžiningai arba tyčia, nėra. Tai reiškia, kad, siekiant įvertinti, ar bankas pagrįstai atsisako kompensuoti pareiškėjos nuostolius, susijusius su Ginčijamų mokėjimų įvykdymu, ir ar galėtų pareiškėjos atžvilgiu būti taikoma Mokėjimų įstatymo 39 straipsnio 3 dalis, būtina nustatyti, ar bankas, kaip mokėjimų paslaugų teikėjas, pateikė pakankamai įrodymų, kurie leistų pagrįstai teigti, kad pareiškėjos elgesys, atskleidžiant personalizuotus jai išduotų mokėjimo priemonių požymius, taip pat kiti veiksmai, dėl kurių galėjo būti įvykdyti Ginčijami mokėjimai, vertintini kaip didelis pareiškėjos neatsargumas, dėl kurio visi jos reikalaujami atlyginti nuostoliai turėtų tekti pačiai pareiškėjai.

Antrosios mokėjimo paslaugų direktyvos (toliau – PSD2) 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 taip pat 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.“[2]

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) 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, išsamiai neįvertinus viso Ginčijamų mokėjimų įvykdymo ir su jais susijusių aplinkybių konteksto.

Sprendimą nekompensuoti pareiškėjos nuostolių bankas grindžia pareiškėjos veiksmais, lėmusiais Ginčijamų mokėjimų įvykdymą, jie, banko vertinimu, rodo pareiškėjos didelį neatsargumą vertinamomis aplinkybėmis. Bankas mano, kad pareiškėja, paspausdama neaiškią nuorodą, suvesdama savo interneto banko ID, asmens kodą ir savo mobiliajame įrenginyje atliekamus veiksmus patvirtindama suvesdama tik jai žinomus Paskyros1 PIN1 ir PIN2 kodus ir dėl to tretieji asmenys pareiškėjos vardu galėjo susikurti Paskyrą2, pažeidė jai, kaip mokėtojai, su mokėjimo priemonės naudojimu nustatytas pareigas ir tai kartu reiškia, kad pareiškėja nesilaikė atidumo ir rūpestingumo reikalavimų.

Vertinamų aplinkybių kontekste visų pirma būtina pažymėti, kad, remiantis pirmiau minėtų Mokėjimų įstatymo nuostatų analize, mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai tik tuo atveju, jei tenkinamos abi sąlygos – 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 pareiškėjos nuostolių dėl neautorizuotų Ginčijamų mokėjimų įvykdymo galėtų būti vertinamas kaip pagrįstas tik tada, jeigu, remiantis banko pateiktais ir ginčo byloje esančiais duomenimis, būtų įrodyta, kad pareiškėja, atskleisdama personalizuotus savo mokėjimo priemonių saugumo duomenis, taip pat suvesdama savo naudojamos „Smart-ID“ Paskyros1 PIN kodus savo mobiliajame įrenginyje ir tokiu būdu įgalindama trečiuosius asmenis panaudoti šiuos duomenis „Smart-ID“ Paskyrai2 sukurti, o vėliau ir inicijuoti bei patvirtinti Ginčijamus mokėjimus, elgėsi itin aplaidžiai – buvo labai neatsargi. Kitaip tariant, specifinis mokėtojo elgesio, kaip labai neatsargaus, vertinimas darytinas atsižvelgus ne į kurią nors vieną aplinkybę, kaip šiuo atveju – aptariamą mokėjimo priemonių personalizuotų saugumo duomenų atskleidimą, tačiau atsižvelgus į tai, kaip konkretaus asmens (mokėtojo) elgesys pasireiškė visų nustatytų aplinkybių kontekste, koks yra žinomas ir (ar) buvo nustatytas nagrinėjant ginčą.

Lietuvos bankas, siekdamas nustatyti, ar pareiškėjos elgesys šiuo atveju gali būti laikomas dideliu neatsargumu, vertino šiuos aspektus: pačios pareiškėjos elgesį pasitikint į telefoną gautame SMS pranešime nurodyta informacija ir spaudžiant jame pateiktą nuorodą, pareiškėjos elgesį, suvedant savo prisijungimo prie interneto banko ir kitus duomenis suklastotame banko interneto banko puslapyje bei suvedant savo naudojamos tapatybės priemonės „Smart-ID“ Paskyros1 PIN1 ir PIN2 slaptažodžius, aktyvavusis „Smart-ID“ programėlei pareiškėjos mobiliajame telefone, taip pat banko veiksmus, kurių jis prevenciškai ėmėsi ir imasi tam, kad mokėjimo paslaugos elektroninėje erdvėje būtų teikiamos saugiai, o pareiškėja būtų tinkamai supažindinta su sukčiavimo elektroninėje erdvėje rizikomis bei

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

tapatybės patvirtinimo priemonės saugaus naudojimo, jos personalizuotų saugumo duomenų suvedimo ir atskleidimo reikšme bei teisinėmis pasekmėmis.

Vertinant pareiškėjos elgesį, svarbu nustatyti, kaip pareiškėja buvo įtikinta atskleisti savo mokėjimo priemonės personalizuotus saugumo bei kitus duomenis tam, kad būtų sukurta „Smart-ID" Paskyra2, įgalinusi trečiuosius asmenis be pareiškėjos žinios ir valinių veiksmų inicijuoti bei patvirtinti Ginčijamus mokėjimus.

Ginčo nagrinėjimo metu buvo nustatyta, kad pareiškėja 2021 m. spalio 21 d. 18:52 val. į savo mobilųjį telefoną, į bendrą kitų iš banko gautų žinučių srautą, gavo trečiųjų asmenų siųstą SMS pranešimą, kuriuo buvo įspėta dėl interneto banko sutarties blokavimo ir paraginta spausti tame pačiame SMS pranešime pateiktą nuorodą: „Jūsų interneto banko sutartis užblokuota apsilankykite seb.login20.com." Gavusi SMS pranešimą, pareiškėja paspaudė jame pateiktą nuorodą *seb.login20.com* ir atsidariusiame trečiųjų asmenų sukurtame interneto tinklalapyje – fiktyvioje banko interneto banko svetainėje, suvedė savo interneto banko atpažinimo kodą (ID), asmens kodą ir savo mobiliajame įrenginyje į savo naudojamą „Smart-ID" Paskyrą1, gavusi patvirtinimo užklausas, suvedė šios paskyros PIN1 ir PIN2 kodus, taip buvo patvirtintas sutikimas pareiškėjos vardu sukurti naują „Smart-ID" paskyrą (Paskyrą2). 18:54 val. bankas apie Paskyros2 sukūrimą informavo pareiškėją SMS pranešimu, išsiųstu į jos mobilųjį telefoną: „Gerb. Kliente, Jūsų vardu SEB banke registruojama „Smart ID Basic" paskyra. Jei to neinicijavote, prašom kuo skubiau susisiekti tel. +370 5 268 2800. SEB bankas." Šią žinutę pareiškėja pripažįsta gavusi, tačiau teigia ją pamačiusi ir perskaičiusi tik po to, kai iš banko gavo antrąją SMS žinutę, perspėjančią apie vykstančią sukčiavimo ataką, ir jau po to, kai Ginčijami mokėjimai buvo įvykdyti.

Tobulėjant technologijoms, tobulėja ir sukčiavimo būdai bei priemonės, sudėtingėja pačios sukčiavimo atakos, todėl jas atpažinti ir nuo jų apsisaugoti reikia vis didesnio mokėjimo paslaugų vartotojų atidumo ir rūpestingumo. Taigi, dėl naujų sukčiavimo būdų, panaudojant naujas technologijas, atsiradimo būtinas itin didelis vartotojų pastabumas ir apdairumas, kuris kartais dėl sukčiavimo atakos naujumo ir kompleksiškumo peržengia net ir vidutinio vartotojo gebėjimą laiku identifikuoti mėginimą neteisėtu būdu pasisavinti mokėjimo priemonę ir (ar) įvykdyti mokėjimo operacijas, kurių mokėjimo paslaugų vartotojas nesiekia įvykdyti. Neabejotina, kad ir šiuo atveju prieš pareiškėją nukreipta sukčiavimo ataka – tapatybės vagystė, t. y. pareiškėjos mokėjimo priemonių personalizuotų saugumo ir pačios pareiškėjos asmens duomenų pasisavinimas tam, kad tretieji asmenys įgytų galimybę sukurti pareiškėjos vardu naują tapatybės patvirtinimo priemonės „Smart-ID" paskyrą ir ja naudodamiesi įgautų prieigą prie pareiškėjos interneto banko, užvaldytų pareiškėjos banko sąskaitas ir inicijuotų bei patvirtintų Ginčijamus mokėjimus, buvo sofistikuota. Naudojantis socialinės inžinerijos metodais, sukurtas tiek poreikis veikti neatidėliotinai tam, kad būtų galima naudotis banko teikiamomis paslaugomis, tiek įtikinamai pasitelkta aplinka (suklastota banko interneto banko svetainė), sukūrusi pirminį tikrumo įspūdį ir skatinusi pasitikėjimą bei mažinusi racionalias, pagrįstas abejones dėl nurodymų atskleisti, suvesti savo mokėjimo priemonių ir asmens duomenis pagrįstumo. Dėl šios priežasties 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 neatskleisti tretiesiems asmenims.

Vertinant banko veiksmus, kurių jis ėmėsi tam, kad informuotų savo klientus, tarp jų ir pareiškėją, apie el. erdvėje kylančias rizikas, naudojantis mokėjimo paslaugomis, pažymėtina, 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 buvusi kokiu nors būdu tinkamai supažindinta su informacija, kokius veiksmus, naudodamasis „Smart-ID" programėle, banko klientas gali atlikti ir kokie veiksmai bei kokiais atvejais, naudojantis šia tapatybės patvirtinimo priemone ir suvedant jos PIN kodus, sukelia atitinkamas teisines pasekmes. 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.“ Nors, kaip teigia bankas, „Smart-ID“ ir nėra banko sukurta tapatybės patvirtinimo priemonė, vis dėlto būtent bankas suteikia galimybę savo klientams (šiuo atveju – pareiškėjai) naudojantis ja nuotoliniu būdu patvirtinti savo tapatybę ir išreikšti savo valią atlikti tam tikrus veiksmus, sukeliančius jiems teisines pasekmes, t. y. naudotis banko teikiamomis paslaugomis – pateikti mokėjimo nurodymą, pasitikrinti sąskaitą ir pan. Tad banko siūlomos ir (ar) leidžiamos naudoti tapatybės patvirtinimo priemonės ne tik turi būti saugios klientams, kurie su banku susiklosčiusiuose sutartiniuose santykiuose naudoja atitinkamą tapatybės patvirtinimo priemonę, bet ir turi būti aiškios: aiškiai pateiktos jos naudojimo sąlygos ir veiksmų, atliekamų su „Smart-ID“, teisinės pasekmės, pavyzdžiui, aiški PIN kodų suvedimo teisinė reikšmė.

Kita vertus, neabejotina ir tai, kad vartotojai, naudodamiesi mokėjimo paslaugomis elektroninėje erdvėje, taip pat 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 vartotojo pareigų, susijusių su mokėjimo priemonių naudojimu, vykdymo. Bankas atsiliepime nurodė, kad klientus nuolat ragina būti budrius ir skelbia aktualią, su sukčiavimo schemomis susijusią informaciją[3]. Be to, bankas apie vykstančią sukčiavimo ataką, dėl kurios nukentėjo ir pareiškėja, taip pat paskelbė savo interneto svetainėje ir išsiuntė pareiškėjai SMS žinutę jos mobiliojo telefono numeriu, tai, kaip minėta, pripažįsta ir pati pareiškėja.

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 apraše, be kita ko, nustatyta, 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 papunktis ir 38 punktas).

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 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.

Įvertinus pirmiau aptartus ginčo bylos duomenis ir ginčo nagrinėjimo metu nustatytas aplinkybes, negalima daryti išvados, kad pareiškėjos elgesys visiškai atitiko banko nustatytas naudojimosi mokėjimo priemonėmis sąlygas ir kad visos pareiškėjai nustatytos pareigos, susijusios su mokėjimo priemonių personalizuotų saugumo duomenų konfidencialumo užtikrinimu, buvo tinkamai įvykdytos. Nors pareiškėjai į mobilųjį telefoną atsiųsta SMS žinutė galėjo sukurti pirminį įspūdį, kad šis pranešimas išsiųstas banko, nes pakliuvo į bendrą kitų iš banko gautų panešimų srautą, tačiau tai, kad pareiškėja iki personalizuotų duomenų atskleidimo (pateikimo suklastotoje interneto svetainėje) nesudvejojo pranešime nurodytos informacijos ir pagal pranešime pateiktą nuorodą atsidariusio interneto puslapio patikimumu,

[3] SEB įspėja: daugėja sukčiavimo skelbimų svetainėse | SEB; https://www.seb.lt/naujienos/2020-09-04/seb-ispeja-suaktyvejo-melagingas-sms-zinutes-platinantys-sukciai ; https://www.seb.lt/infobankas/kasdieniai-finansai/nusikalteliai-internete-tobuleja-ka-gali-nuveikti-turedami-jusu.

taip pat nekvestionuodama pateiktų nurodymų pagrįstumo suvedė savo naudojamos „Smart-ID" Paskyros1 PIN1 ir PIN2 slaptažodžius, atsiradus tai padaryti raginantiems „Smart-ID" programėlės pranešimams, leidžia teigti, kad pareiškėjos elgesys aptariamų aplinkybių metu nebuvo itin apdairus ir atsargus. Duomenų, kad anksčiau pareiškėja vuvo gavusi banko siųstų žinučių su aktyviomis nuorodomis į banko interneto svetainę ar banko interneto banką, ginčo byloje nėra.

Verta atkreipti dėmesį ir į tai, kad, kaip jau minėta, 2021 m. spalio 21 d. 18:54 val. bankas apie Paskyros2 sukūrimą pareiškėjos vardu informavo pareiškėją SMS pranešimu, išsiųstu į pareiškėjos mobilųjį telefoną: „Gerb. Kliente, Jūsų vardu SEB banke registruojama „Smart ID Basic" paskyra. Jei to neinicijavote, prašom kuo skubiau susisiekti tel. +370 5 268 2800. SEB bankas." Bankas kartu su atsiliepimu pateikė duomenis, kad minėta žinutė buvo išsiųsta pareiškėjai jos mobiliojo telefono numeriu. Pati pareiškėja taip pat pripažįsta banko siųstą SMS žinutę, informuojančią pareiškėją apie jos vardu sukurtą „Smart-ID" Paskyrą2, gavusi, tačiau nurodo laiku (t. y. kai žinutė buvo gauta ir (ar) iki įvykdant Ginčijamus mokėjimus) jos neperskaičiusi. Be to, bankas pateikė duomenis, kad pranešimą, informuojantį pareiškėją apie jos vardu sukurtą „Smart-ID" Paskyrą2, pareiškėjos el. pašto adresu siuntė ir SK, pranešime nurodydama: „Saugumo pranešimas: buvo sukurta nauja Smart ID paskyra!"

Kaip aplinkybę, pagrindžiančią bankui keliamą reikalavimą, pareiškėja įvardija faktą, kad pirmasis Ginčijamas mokėjimas buvo įvykdytas 19.07 val., o banko siųstą SMS pranešimą, įspėjantį apie vykstančią sukčiavimo ataką, ji gavo tik 20.01 val. – praėjus daugiau nei valandai nuo sukčių siųsto SMS pranešimo ir naujos „Smart-ID" paskyros sukūrimo pareiškėjos vardu. Taigi, pareiškėja mano, kad jei minėtą banko pranešimą ji būtų gavusi anksčiau, ji nebūtų tapusi sukčių auka ir praradusi visų savo gyvenimo santaupų. Vis dėlto, kaip minėta, pirmiau nei banko SMS pranešimą, įspėjantį apie vykstančią sukčiavimo ataką, pareiškėja gavo tiek banko, tiek SK siųstus pranešimus, informuojančius pareiškėją apie jos vardu sukurtą „Smart-ID" Paskyrą2, tačiau šių pranešimų laiku (t. y. iki įvykdant Ginčijamus mokėjimus) pareiškėja neperskaitė. Ginčo nagrinėjimo metu nenustatyta duomenų, kad egzistuotų priežastinis ryšys tarp įspėjančio apie sukčiavimo ataką banko SMS pranešimo išsiuntimo laiko (vėlesnio nei pačios prieš pareiškėją įvykdytos sukčiavimo atakos laikas) ir pareiškėjos nuostolių dėl Ginčijamų mokėjimų įvykdymo, taigi, kad banko SMS žinutės, įspėjančios apie vykstančią sukčiavimo ataką, ankstesnis išsiuntimas tikrai būtų apsaugojęs pareiškėją nuo „Smart-ID" Paskyros2 sukūrimo.

Kita vertus, kaip minėta, remiantis Mokėjimų įstatymo 39 straipsnio 3 dalies nuostatomis, mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai, jeigu jis juos patyrė veikdamas ne tik neatsargiai, bet ir dėl didelio neatsargumo neįvykdęs vienos ar kelių Mokėjimų įstatymo 34 straipsnyje nustatytų pareigų. Vadinasi, išvada dėl mokėtojo buvimo nepakankamai apdairiu ar atsargiu arba, kitaip tariant, išvada, kad mokėtojas buvo tik nepakankamai apdairus ir rūpestingas ar net neatsargus, yra nepakankama tam, kad būtų taikoma Mokėjimų įstatymo 39 straipsnio 3 dalis. Pagal šią Mokėjimų įstatymo nuostatą, dėl neautorizuotų mokėjimo operacijų kilę nuostoliai tenka pačiam mokėtojui, jei mokėtojas, veikdamas nesąžiningai arba tyčia ar dėl *didelio* neatsargumo, neįvykdo jam Mokėjimų įstatyme ir sutartyje su mokėjimo paslaugų teikėju nustatytų pareigų.

Bankas atsiliepime teigia, kad pareiškėja turėjo naudojimosi „Smart-ID" programėle, kaip tapatybės patvirtinimo priemone, patirties, tad, šiuo atveju suvesdama savo naudojamos „Smart-ID" Paskyros1 PIN1 ir PIN2 kodus, šios programėlės atsiradusių pranešimų languose galėjo ir turėjo matyti prašomus atlikti veiksmus (PIN1 ir PIN2 kodų suvedimą) identifikuojančius žodžius „Prisijungimas" arba „Login", „Patvirtinimas", kurie nurodė, kad PIN1 ir PIN2 kodų suvedimu patvirtinami prisijungimo, tapatybei identifikuoti reikalingi veiksmai. Tad, banko vertinimu, pareiškėjai turėjo būti žinoma ir suprantama, kokiu tikslu jos prašoma suvesti „Smart-ID" Paskyros1 PIN1 ir PIN2 kodus.

Vis dėlto šie banko argumentai vertintini kritiškai: nors pareiškėja turėjo naudojimosi „Smart-ID" programėle patirties ir jai buvo žinoma, kad naudojantis šia tapatybės patvirtinimo priemone pareiškėja gali prisijungti prie interneto banko, tvirtinti inicijuotus mokėjimo nurodymus įvykdyti mokėjimo operacijas, atlikti interneto banke kitus šalių sutartus veiksmus, sukeliančius teisines pasekmes pareiškėjai (pavyzdžiui, sudaryti ar nutraukti sutartis ir pan.), tačiau šiuo konkrečiu atveju pareiškėja paspaudė sukčių atsiųstame SMS pranešime pateiktą nuorodą, suvedė savo prisijungimo prie interneto banko duomenis, o vėliau (telefone pasirodžius „Smart-ID" programėlės pranešimams) suvedė savo naudojamos „Smart-ID" Paskyros1 PIN1 ir PIN2 kodus, tikėdama, kad taip atlieka veiksmus savo tapatybei identifikuoti

tam, kad prisijungtų prie savo interneto banko (PIN1 kodo suvedimu), o vėliau tvirtina veiksmus, kuriais pašalinamos kliūtys, problemos, lėmusios tariamą interneto banko sutarties (prieigos prie interneto banko) užblokavimą (PIN2 kodo suvedimu). Paaiškinimuose dėl „Smart-ID" Paskyros1 PIN2 kodo suvedimo aplinkybių (t. y. suvedimo tikslo) ir (ar) vaizdų, kuriuos pareiškėja matė savo mobiliojo telefono ekrane suklastotoje banko interneto banko svetainėje prieš pat atsirandant „Smart-ID" Paskyros1 pranešimui suvesti PIN2 kodą, pareiškėja nurodė, kad suklastotos banko interneto banko svetainės vaizdų ji nėra išsaugojusi. Vis dėlto pareiškėja kartu pažymėjo, kad „<...> paklausimas suvesti PIN2 kodą, nepasirodė neįprastas. <...> Mano atveju atrodė logiška, nes žinutėje buvo pranešimas, kad sutartis užblokuota, tai ir prašymas suvesti abu kodus, neatrodė įtartinas. Suvedus, atsidarė paskyra, ir tarsi logiškas buvo patvirtinimas, kad viskas veikia." Taigi, galima teigti, kad pareiškėja suprato Paskyros1 PIN1 ir PIN2 kodų suvedimo paskirtį būtent taip, kaip įprastai šie kodai ir naudojami – patvirtinti prisijungimą prie savo paskyros (PIN1 kodo suvedimu) ir patvirtinti atitinkamą veiksmą (šiuo atveju panaikinti sutarties (prieigos prie interneto banko) užblokavimą) (PIN2 kodo suvedimu). Pagal viešai prieinamas „Smart-ID" naudojimo sąlygas vertinant aplinkybę, kad PIN2 kodas yra naudojamas ne tik mokėjimo operacijai patvirtinti, bet ir atitinkamiems susitarimams patvirtinti, pareiškėjai pagrįstai galėjo atrodyti, kad sutarties (prieigos prie interneto banko) užblokavimo problema suvedant PIN2 kodą yra normalus veiksmas, kuriuo patvirtinamas sutikimas panaikinti minėtą užblokavimą.

Būtina atkreipti dėmesį ir į tai, kad, banko pateiktais duomenimis[4], „Smart-ID" Paskyros1 pranešimuose, kuriais pareiškėjos buvo prašoma suvesti PIN1 ir PIN2 kodus, be kontrolinio kodo, buvo rodomi tik pirmiau minėti prašomus atlikti veiksmus identifikuojantys bendro pobūdžio reikšmę turintys žodžiai „Prisijungimas" (suvedant PIN1 kodą) ir „Patvirtinimas" (suvedant PIN2 kodą), jokiais papildomais požymiais neaprašant, nedetalizuojant veiksmo, kuriam tvirtinti prašoma suvesti PIN2 kodą (pvz., kad šį kodą prašoma suvesti norint patvirtinti mokėjimo operaciją ar pan.). Taigi, banko vertinimo, kad pareiškėja matė ir suprato ar turėjo suprasti, kokiam veiksmui iš tiesų išreiškia sutikimą, suvesdama „Smart-ID" Paskyros1 PIN2 kodą, nepagrindžia ginčo nagrinėjimo metu nustatyti ir pirmiau aptarti duomenys. Kitaip tariant, pareiškėjos teigimu, pagal SMS žinutėje pateiktą nuorodą atsidariusioje suklastotoje banko interneto banko svetainėje pareiškėja siekė prisijungti prie savo interneto banko paskyros tam, kad vėliau, paisydama minėtos žinutės įspėjimų, atliktų, patvirtintų veiksmus, kuriais atblokuojama tariamai užblokuota jos interneto banko paskyra. Remiantis ginčo byloje esančiais įrodymais, kitų duomenų, kurie leistų teigti, kad pareiškėja galėjo ir turėjo matyti bei suprasti suvedamų duomenų ir programėlės „Smart-ID" Paskyros1 PIN kodų tikrąjį tikslą ir pasekmes, nėra.

Paaiškinimuose dėl savo veiksmų, atskleidžiant prisijungimo prie savo interneto banko bei kitus duomenis suklastotoje interneto svetainėje, paspaudus trečiųjų asmenų siųstame SMS pranešime pateiktą nuorodą, pareiškėja atkreipia dėmesį, kad minėta trečiųjų asmenų siųsta žinutė pakliuvo į bendrą kitų iš banko gautų autentiškų žinučių srautą, ir tai sumažino pareiškėjos budrumą, ypač dėl to, kad dienos metu „Smart-ID" programėlė neveikė sklandžiai, tad žinutės turinys pareiškėjai nepasirodė įtartinas[5]. Pareiškėjos teigimu, jei tokia žinutė nebūtų pakliuvusi į kitų iš banko gautų žinučių srautą arba sukčiai būtų paskambinę pareiškėjai telefonu, pareiškėjos atsargumas nebūtų buvęs paveiktas ir ji nebūtų sureagavusi į prašymus atskleisti savo mokėjimo priemonių personalizuotus saugumo duomenis bei suvesti „Smart-ID" Paskyros1 slaptažodžius.

Vertinant pareiškėjos neatsargumo laipsnį, svarbu tai, kad trečiųjų asmenų pareiškėjai siųsta SMS žinutė su nuoroda į suklastotą banko interneto svetainę ne tik pakliuvo į bendrą kitų banko pareiškėjai siųstų žinučių srautą, tačiau ir buvo parašyta lietuviškais rašmenimis[6]. Be to, pačios nuorodos pavadinimas (t. y. suklastotos interneto svetainės adresas) *seb.login20.com* turėjo klaidinantį panašumą į tikrąjį banko interneto svetainės adresą: nuorodos į suklastotą

[4] Bankas su papildomais paaiškinimais pateikė duomenis, kokio turinio „Smart-ID" pranešimai, prašantys suvesti PIN1 ir PIN2 kodus buvo siunčiami banko klientams, taigi, ir pareiškėjai, tuo metu, kai buvo sukurta „Smart-ID" Paskyra2 ir įvykdyti Ginčijami mokėjimai.

[5] Bankas atsiliepime paaiškino, kad šiuolaikinės technologijos įgalina asmenis, tarp jų ir sukčius, iš tam tikrų platformų siųsti SMS žinutes nurodžius bet kokį siuntėjo vardą. Kaip nurodo bankas, mobilieji telefonai įprastai SMS žinutes grupuoja pagal siuntėjo vardą, todėl tokia žinute dėl jos sugrupavimo telefone su ankstesniu tikru susirašinėjimu su banku siekiama sukelti pasitikėjimą gavėjui sudarant įspūdį, kad ji gauta neva iš banko, taip įvyko ir pareiškėjos atveju.

[6] Remiantis ginčų nagrinėjimo panašiose ginčo bylose (t. y. ginčo bylose dėl neautorizuotų mokėjimo operacijų, įvykus sukčiavimo atakai) praktika, galima teigti, kad sukčių vartotojams siunčiamos SMS žinutės, raginančios paspausti nuorodą į suklastotas interneto svetaines, dažniausiai būna parašytos nelietuviškais rašmenimis.

interneto svetainę pavadinime vartojami žodžiai „Seb“ (pats banko pavadinimas), „login“ („log in“ iš anglų k. – „prisijungti“), „.com“ – visuotinai priimtina patikimų interneto svetainių adresų pabaiga, kuri pareiškėjai, jos teigimu, sukūrė tikrumo ir patikimumo įspūdį, arba tiksliau – nesukėlė abejonių, kad nuoroda iš tiesų nukreipia ne į tikrąją, o suklastotą banko interneto banko svetainę. Dėl nurodytų priežasčių tam, kad būtų galima suabejoti pareiškėjai trečiųjų asmenų siųstos žinutės turinio ir joje pateitos nuorodos patikimumu, atsižvelgiant ir į tai, kad, kaip teigia pareiškėja, atsidariusi suklastota banko interneto svetainė (vizualine prasme) buvo identiška tikrajai banko interneto banko svetainei, buvo būtinas itin didelis vartotojo pastabumas ir informuotumas, taigi, konkrečios žinios, kada ir kaip panašaus pobūdžio sukčiavimo atakos gali įvykti. Vis dėlto tokių duomenų ginčo nagrinėjimo metu nenustatyta, kaip ir duomenų, kad pareiškėja matė ir turėjo suprasti, kokiu tikslu atskleidžia savo prisijungimo prie interneto banko duomenis ir suveda savo „Smart-ID“ Paskyros1 PIN kodus.

Pagrįsdamas savo sprendimą nekompensuoti pareiškėjos nuostolių, susijusių su Ginčijamų mokėjimų įvykdymu, bankas taip pat akcentuoja, kad elektroninio parašo „Smart-ID“ ir „Smart-ID Basic“ leidėjas yra ne bankas, o SK, kuri nustato „Smart-ID“ ir „Smart-ID Basic“ išdavimo ir naudojimo sąlygas, ir šios sąlygos, kaip ir pats „Smart-ID“ paskyrų kūrimas, nėra susijusios su mokėjimo paslaugų teikimu.

Atsižvelgiant į šiuos banko teiginius, vis dėlto būtina pažymėti, kad ši specifinė prieš pareiškėją nukreipta sukčiavimo ataka – naujos „Smart-ID“ paskyros pareiškėjos vardu sukūrimas, taip neteisėtai pasisavinant pareiškėjos tapatybę, o galiausiai ir jos mokėjimo priemonę (prieigą prie interneto banko) ir inicijuojant bei patvirtinant Ginčijamus mokėjimus, nebuvo savitikslė. Šiuo atveju tretieji asmenys, kaip galima numanyti, neteisėtu būdu iš pareiškėjos išvilioję jos prisijungimo prie interneto banko duomenis, vėliau pareiškėjai dėl trečiųjų asmenų apgaulės suvedus jos naudojamos „Smart-ID“ Paskyros1 PIN kodus savo mobiliajame įrenginyje esančioje programėlėje „Smart-ID“, įgavo ne tik galimybę sukurti naują „Smart-ID“ Paskyrą2 pareiškėjos vardu, bet ir (ginčo bylos duomenimis) atliko šiuos veiksmus vienu konkrečiu tikslu – tam, kad įgautų prieigą prie pareiškėjos interneto banko ir naudodamiesi „Smart-ID“ Paskyra2, kaip elektroniniu parašu, užvaldytų pareiškėjos banko sąskaitose esančias lėšas, įvykdydami pareiškėjos neautorizuotus Ginčijamus mokėjimus, tikėtina, būtent trečiųjų asmenų ar su jais susijusių subjektų naudai. Dėl nurodytų priežasčių „Smart-ID“ Paskyros2 sukūrimo aplinkybės yra itin reikšmingos, vertinant pareiškėjos reikalavimo bankui pagrįstumą – nors „Smart-ID“ ar „Smart-ID Basic“ ir nėra banko teikiama paslauga, tačiau būtent bankas suteikia galimybę savo klientams (šiuo atveju – pareiškėjai) sutartiniuose santykiuose su banku, taigi, naudojantis ir banko teikiamomis mokėjimo paslaugomis, naudotis programėle „Smart-ID“, kaip tinkama tapatybės patvirtinimo priemone inicijuojant ir tvirtinant mokėjimus, tai būtent ir darė pareiškėja, naudodamasi savo „Smart-ID“ Paskyra1. Kaip jau buvo minėta pirmiau, banko siūlomos ir (ar) leidžiamos naudoti tapatybės patvirtinimo priemonės turi būti ne tik saugios klientams, kurie su banku susiklosčiusiuose sutartiniuose santykiuose naudoja atitinkamą tapatybės patvirtinimo priemonę, bet ir aiškiai pateiktos jos naudojimo sąlygos bei su ja atliekamų veiksmų teisinės pasekmės. Kita vertus, „Smart-ID“, kaip tapatybės patvirtinimo priemonės, nesąžiningo (neteisėto) naudojimo ir (ar) pasisavinimo aplinkybės vertinamos tik tiek, kiek jos lemia neautorizuotų mokėjimo operacijų įvykdymą, ir yra reikšmingos tiek, kad būtų galima įvertinti mokėtojo elgesio atitiktį rūpestingumo standartams ir nustatytoms pareigoms, susijusioms su mokėjimo priemonių naudojimu. Duomenų, kad bankas būtų aiškiai ir tinkamai supažindinęs pareiškėją su „Smart-ID“ PIN kodų suvedimo reikšme ir teisinėmis pasekmėmis tarp šalių susiklosčiusiuose santykiuose, tarp jų ir bankui teikiant mokėjimo paslaugas pareiškėjai, kaip jau minėta, ginčo byloje nėra.

Be to, verta paminėti ir tai, kad, laikantis banko išsakytos pozicijos, kad „Smart-ID“ Paskyros2 sukūrimo aplinkybės nėra susijusios su mokėjimo paslaugų teikimu, tad jos neturėtų būti vertinamos sprendžiant dėl banko pareigos grąžinti ir (ar) kompensuoti pareiškėjai Ginčijamų mokėjimų sumą, reikėtų kartu savaime konstatuoti ir tai, kad pareiškėjos Ginčijami mokėjimai, kaip nustatyta ginčo nagrinėjimo metu ir to neginčija bankas, yra neautorizuoti mokėjimai, įvykdyti trečiųjų asmenų be pareiškėjos žinios ir jos valinių veiksmų, tad nuostolius dėl tokių neautorizuotų mokėjimų turėtų kompensuoti bankas Mokėjimų įstatymo 38 straipsnio 1 dalies ir 39 straipsnio 1 bei 2 dalyse nustatyta tvarka. Kitaip tariant, laikantis banko pozicijos, įvykus analogiškoms kaip nagrinėjamo ginčo atveju sukčiavimo atakoms, vartotojų ginčijamų kaip neautorizuotų mokėjimų sumos turėtų būti grąžinamos vartotojams be papildomo jų elgesio (ne)atsargumo vertinimo, kaip tai nustatyta Mokėjimų įstatyme.

Įvertinęs visas pirmiau nurodytas aplinkybes, susijusias su naujos „Smart-ID" Paskyros2 pareiškėjos vardu sukūrimu ir vėliau lėmusias pareiškėjos neautorizuotų Ginčijamų mokėjimų įvykdymą, taip pat banko pateiktus duomenis, kuriais jis grindžia atsisakymą grąžinti pareiškėjai Ginčijamų mokėjimų sumas dėl jos didelio neatsargumo, Lietuvos bankas daro išvadą, kad vis dėlto vertinti pareiškėjos elgesį, dėl kurio ji prarado savo mokėjimo priemonę – prieigą prie savo interneto banko, kaip elgesį, pasireiškusį neprotingumu ar išskirtiniu rūpestingumo nebuvimu, nėra pagrindo. Lietuvos banko vertinimu, šiuo konkrečiu atveju sukčių suklastota SMS žinutė, pakliuvusi į bendrą kitų iš banko gautų SMS žinučių srautą, formos ir turinio prasme buvo pateikta taip, kad galėjo pagrįstai sudaryti įspūdį, kad tai paties banko siųstas pranešimas, o minėtoje SMS žinutėje pateikta nuoroda į suklastotą banko interneto banko svetainę, taip pat ir, pareiškėjos teigimu, pati suklastota banko interneto banko svetainė buvo klaidinamai panašios į autentišką banko interneto banko svetainės adresą ir pačią interneto svetainę. Be to, įvertinus tai, kad „Smart-ID" Paskyros1 pranešimuose, kuriais pareiškėjos buvo prašoma suvesti PIN1 ir PIN2 kodus, be kontrolinio kodo, buvo rodomi tik pirmiau minėti prašomus atlikti veiksmus identifikuojantys bendro pobūdžio reikšmę turintys žodžiai „Prisijungimas" (suvedant PIN1 kodą) ir „Patvirtinimas" (suvedant PIN2 kodą), manytina, kad pareiškėjai pagrįstai galėjo susidaryti įspūdis, kad ji, kaip tuo metu tikėjo, vykdydama banko nurodymus, atlieka veiksmus, kurie įprastai atliekami tam, kad pareiškėjos prieiga prie interneto banko paskyros būtų atblokuota.

Vertinant Mokėjimų įstatymo nuostatas, reglamentuojančias atsakomybės už neautorizuotų mokėjimo operacijų įvykdymą pasiskirstymą, tam, kad bankas būtų atleistas nuo pareigos grąžinti neautorizuotų mokėjimo operacijų lėšas, bankas, kaip pareiškėjos mokėjimo paslaugų teikėjas, turėjo pateikti įrodymų, pagrindžiančių pareiškėjos sukčiavimą arba didelį neatsargumą. Pirmiau konstatuota, kad, Lietuvos banko nuomone, bankas šiuo atveju nepateikė pakankamai pagrįstų įrodymų, kad pareiškėjos elgesys, dėl kurio ji prarado savo mokėjimo priemonę, turėtų būti laikomas ne tik neatsargiu, bet ir išskirtinai neprotingu bei labai neatsargiu. Duomenų apie galimą pareiškėjos sukčiavimą ar kitokį nesąžiningą veikimą ginčo byloje nėra. Kitų aplinkybių, kurios leistų pagrįstai manyti, kad pareiškėjai turėtų tekti visi su neautorizuotomis mokėjimo operacijomis – Ginčijamais mokėjimais, susiję nuostoliai, ginčo byloje taip pat nenustatyta, todėl, įvertinus pirmiau išdėstytą informaciją, konstatuotina, kad pagrindo pareiškėjai taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį nėra.

Tačiau Mokėjimų įstatymo 39 straipsnio 2 dalyje nustatyta, kad mokėtojas neturi patirti jokių nuostolių, jeigu jis iki mokėjimo operacijos įvykdymo negalėjo pastebėti mokėjimo priemonės praradimo, vagystės arba neteisėto pasisavinimo, išskyrus atvejus, kai jis veikė nesąžiningai (1 punktas). Vis dėlto, nors pareiškėjos elgesys, dėl kurio ji prarado savo mokėjimo priemonę, nebuvo labai neatsargus, tačiau nustatyti duomenys ir aplinkybės sudaro pagrindą teigti, kad pareiškėja iki Ginčijamų mokėjimų įvykdymo turėjo galimybę pastebėti, kad jos mokėjimo priemonę pasisavino tretieji asmenys. Tiek bankas, tiek tapatybės patvirtinimo priemonės leidėja SK dar iki 19:07 val. įvykusio Ginčijamų mokėjimų inicijavimo ir įvykdymo 18:54 val. informavo pareiškėją, kad jos vardu kuriama nauja „Smart-ID" paskyra ir kad jeigu pareiškėja to neinicijavo, kuo skubiau susisiektų su banku. Nors „Smart-ID" paskyra savo esme yra SK sukurta tapatybės patvirtinimo priemonė, o ne banko išduodama mokėjimo priemonė, tačiau šiuo konkrečiu atveju, įvertinus į pareiškėją nukreiptos sukčiavimo atakos pobūdį ir tai, kam, kokiu tikslu „Smart-ID" Paskyra2 pareiškėjos vardu buvo sukurta, taip pat atsižvelgiant į tai, kad pati pareiškėja „Smart-ID" Paskyrą1 naudojo prieigai prie savo interneto banko ir mokėjimo operacijoms autorizuoti, neabejotina, kad informacija apie naujos „Smart-ID" paskyros sukūrimą turėjo suteikti rimtą pagrindą abejonei, kad pareiškėjos turima mokėjimo priemonė (-ės) galėjo būti prarasta ar neteisėtai pasisavinta, tai patvirtina ir pareiškėjos kreipimesi dėstomos ginčo aplinkybės[7]. Vadinasi, pareiškėja dar iki Ginčijamų mokėjimų įvykdymo turėjo galimybę pastebėti savo mokėjimo priemonės – prieigos prie interneto banko, galimą neteisėtą pasisavinimą, nes nuo informacijos apie kuriamą naują Paskyrą2 iki Ginčijamų mokėjimų įvykdymo praėjo apie 13 min. Ši aplinkybė, taip pat pirmiau analizuotos ir vertintos aplinkybės, susijusios su pareiškėjos elgesiu, dėl kurio tretieji asmenys įgijo galimybę inicijuoti ir įvykdyti pareiškėjos neautorizuotas mokėjimo operacijas, leidžia konstatuoti, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 1 dalį, pagal kurią

[7] Pareiškėja kreipimesi teigia: „kai pamačiau, paskutinį pranešimą iš banko SMS 20.01 nepatikėjau savo akimis, buvo tekstas vyksta SMS sukčių ataka. Nespauskite gautų nuorodų ir neatskleiskite savo duomenų. Paskambinus +370 5 268 2800, sužinojau apie sukčiavimo aktus, kurie galėtų išmušti ir patį stipriausią žmogų, sužinojus, kad dingo viso gyvenimo santaupos."

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. Lietuvos banko vertinimu, šiuo atveju pareiškėjos reikalavimas bankui grąžinti ir (ar) kompensuoti jai Ginčijamų mokėjimų sumą turėtų būti tenkinamas iš dalies, vertinant, kad bankas turėtų grąžinti pareiškėjai Ginčijamų mokėjimų sumą, išskaičius pareiškėjos atsakomybei tenkančią 50 Eur sumą, taigi, iš viso 32 286 Eur.

Dėl banko teikiamų mokėjimo paslaugų saugumo

Pareiškėja, grįsdama bankui keliamą reikalavimą dėl nuostolių, susijusių su Ginčijamų mokėjimų įvykdymu, kompensavimo, be kita ko, teigia, kad bankas nesiėmė reikiamų veiksmų, kad užtikrintų pareiškėjos banko sąskaitose esančių lėšų saugumą.

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, kad bankas nesiėmė reikiamų veiksmų tam, kad būtų apsaugotas jos banko sąskaitos ir joje esančių lėšų saugumas, ir kad įvykdydamas Ginčijamus mokėjimus bankas būtų pažeidęs finansų rinką reglamentuojančių teisės aktų reikalavimus.

Paaiškinimuose dėl pareiškėjos teiginių, kad Ginčijamų mokėjimų įvykdymo dieną „Smart-ID" programėlė, siekiant atlikti mokėjimus, prisijungus prie interneto banko, neveikė sklandžiai, bankas taip pat pažymėjo, kad vykdant Ginčijamus mokėjimus nebuvo užfiksuota banko sistemų sutrikimų ar sulėtėjimo, bankas taip pat negavo pranešimų iš SK apie „Smart-ID" programėlės veikimo sutrikimus.

Kaip papildomą aplinkybę, pagrindžiančią abejonę dėl banko teikiamų mokėjimo paslaugų saugumo, pareiškėja nurodo tai, kad bankas jos, kaip klientės, nėra įspėjęs apie nustatytus dienos ir mėnesio operacijų limitus ir (ar) rekomendavęs juos nusistatyti minimalius, t. y. tik tokio dydžio, kiek iš tiesų būtina dienos ir mėnesio operacijoms atlikti. Atsižvelgdamas į šį pareiškėjos teiginį, bankas paaiškino, kad klientus nuolat ragina nusistatyti minimalius reikiamus mokėjimų operacijų limitus ir, atlikus didesnius mokėjimus, kuriems yra reikalingi didesni mokėjimo operacijų limitai, juos vėl grąžinti į minimalius. Kita vertus, atsiliepime nurodoma, kad pareiškėjos banko sąskaitoms, iš kurių buvo atlikti Ginčijami mokėjimai, yra nustatyti 20 000 Eur dienos ir 20 000 Eur mėnesio operacijų limitai. Bankas atkreipė dėmesį, kad tokio dydžio mokėjimo operacijų limitų pageidavo pati pareiškėja ir dėl jų dydžio susitarė su banku 2020 m. rugpjūčio 10 d. šalių sudarytoje Interneto banko sutartyje.

Pažymėtina, kad vien aplinkybė, jog Ginčijami mokėjimai buvo įvykdyti, 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 tiek naujos „Smart-ID" paskyros pareiškėjos vardu sukūrimą, tiek ir pačių Ginčijamų mokėjimų įvykdymą.

Kita vertus, ginčo nagrinėjimo metu konstatuota, kad nors pareiškėjos elgesys nelaikytinas itin atidžiu ir apdairiu, vis dėlto jis negali būti vertinamas ir kaip toks neatsargus, kad būtų akivaizdžiai neprotingas ir neatitikantis elementarių rūpestingumo standartų, dėl to visi neautorizuotų Ginčijamų mokėjimų nuostoliai turėtų tekti pačiai pareiškėjai. Nenustačius pareiškėjos didelio neatsargumo dėl „Smart-ID" Paskyros2 sukūrimo, lėmusio Ginčijamų mokėjimų įvykdymą, kaip minėta, nėra teisinio pagrindo pareiškėjos atžvilgiu taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį. Todėl pareiškėjos nuostoliai dėl Ginčijamų mokėjimų įvykdymo, vadovaujantis pirmiau išdėstytais argumentais, turėti būti paskirstyti atsižvelgiant į Mokėjimų įstatymo 39 straipsnio 1 dalį, t. y. iš grąžintinų Ginčijamų mokėjimų sumos, išskaičius pareiškėjos atsakomybei tenkančią 50 Eur sumą.

Remdamasis tuo, kas išdėstyta, ir vadovaudamasis Vartotojų teisių apsaugos įstatymo 27 straipsnio 1 dalies 1 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 59.2 papunkčiu, n u s p r e n d ž i u:

1. Iš dalies tenkinti pareiškėjos reikalavimą ir rekomenduoti bankui kompensuoti

pareiškėjai 32 286 Eur sumą.

2. Įpareigoti banką per mėnesį nuo šio sprendimo priėmimo dienos raštu informuoti Lietuvos banką apie šio sprendimo rezoliucinės dalies 1 punkte nurodytos rekomendacijos įgyvendinimą (neįgyvendinimą). Bankui neįvykdžius minėtos rekomendacijos, apie tai bus paskelbta Lietuvos Respublikos teisės aktų nustatyta tvarka.

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