LIETUVOS BANKO PRIEŽIŪROS TARNYBOS TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

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

2020 m. gruodžio 16 d. Nr. V 2020/(34.70.E-3403)-429-50
Vilnius

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

Nustatyta:

2020 m. rugsėjo 7 d. 22:14 val. pareiškėja į savo telefono numerį gavo, kaip vėliau paaiškėjo, suklastotą SMS žinutę su pranešimu „Atnaujinkite „SmartID" paskyrą"[1]. Minėta SMS žinutė buvo siųsta iš telefono numerio, nesusieto su banku, joje buvo pateikta aktyvi nuoroda. Pareiškėja teigė, kad, paspaudusi SMS žinute atsiųstą nuorodą, pateko į, kaip vėliau paaiškėjo, suklastotą banko internetinės bankininkystės puslapį, vizualiai panašų į įprastą puslapį. Pareiškėjai į suklastotą banko internetinės bankininkystės puslapį suvedus banko jai suteiktą naudotojo ID numerį (toliau – banko ID) ir savo asmens kodą, pareiškėjos telefone buvo aktyvuota programėlė „SmartID" (toliau – „SmartID"). Pareiškėja šioje programėlėje suvedė PIN1 ir PIN2 kodus, galvodama, kaip ji teigia, kad taip atnaujina „SmartID" paskyrą. Tačiau iš tikrųjų buvo duotas sutikimas iš pareiškėjos banko sąskaitos 2020 m. rugsėjo 7 d. 22:41:25 val. įvykdyti mokėjimo nurodymą – 1 000 Eur sumą pervesti gavėjui *A DOBRE.* Mokėjimo operacija buvo įvykdyta kaip momentinis mokėjimas. 22:41:27 val. bankas pareiškėjos telefone „SmartID" programėlėje parodė pranešimą, kad yra įvykdytas 1 000 Eur mokėjimas gavėjui *A DOBRE.* Tik tada pareiškėja suprato, kad buvo apgauta, o 1 000 Eur iš jos banko sąskaitos pasisavinti neteisėtu būdu. Pareiškėja iš karto telefonu kreipėsi į banką dėl mokėjimo priemonės blokavimo. Pareiškėjos ir banko pokalbio pradžia – 22:45:35 val., mokėjimo priemonė užblokuota – 22:48:43 val.

2020 m. rugsėjo 8 d. pareiškėja pateikė bankui prašymą grąžinti 1 000 Eur. Bankas pareiškėjai 2020 m. rugsėjo 9 d. pateiktame atsakyme nurodė nesutinkantis grąžinti 1 000 Eur, nes bankui pateikta vykdyti mokėjimo operacija buvo patvirtinta tik pareiškėjai asmeniškai žinomomis tapatybės patvirtinimo priemonėmis (banko ID, asmens kodu bei PIN slaptažodžiais), todėl bankas ją tinkamai įvykdė. Bankas pareiškėjai nurodė, kad, banko sistemų turimais duomenimis, bankas prieš pareiškėjai „SmartID" suvedant PIN2 kodą rodė informaciją, kad yra tvirtinamas 1 000 Eur mokėjimo pavedimas gavėjui *A DOBRE*. Bankas pareiškėjai paaiškino, kad jeigu ji prieš suvesdama PIN2 kodą šios informacijos neperskaitė, toks jos elgesys yra vertinamas didelis neatsargumas. Taip pat bankas informavo pareiškėją, kad kreipėsi į gavėjo banką dėl mokėjimo operacijos atšaukimo.

2020 m. rugsėjo 16 d. pareiškėja kreipėsi į Lietuvos banką dėl vartojimo ginčo nagrinėjimo ir prašė rekomenduoti bankui grąžinti neteisėtu būdu iš jos banko sąskaitos nurašytus 1 000 Eur. Kreipimesi pareiškėja išdėstė pirmiau aprašytas aplinkybes, kaip buvo pateiktas vykdyti 1 000 Eur mokėjimo nurodymas, ir pažymėjo, kad prieš suvesdama PIN2 kodo slaptažodį jokio banko pranešimo, kad bus daromas 1 000 Eur pavedimas, negavo. Pareiškėja pažymėjo, kad bankas yra įsipareigojęs saugoti jos pinigus, todėl bankas turėjo apsaugoti pareiškėjos banko sąskaitą nuo trečiųjų šalių patekimo į ją. Pareiškėjos teigimu, bankas neužtikrino, kad į banko interneto banko aplinką būtų galima patekti tik per banko

[1] „SmartID" – tai trečiosios šalies („SK ID Solutions AS") teikiama programėlė (aplikacija), atliekanti el. parašo ir el. atpažinties funkcijas. Lietuvoje veikiantys bankai šią programėlę laiko pagrindine priemone mokėjimo operacijoms autorizuoti, sutartims pasirašyti ar kitoms su banko veikla susijusioms operacijoms tvirtinti.

interneto puslapį, taip pat neužtikrino ir to, kad į „SmartID“ programėlę nepatektų tretieji asmenys.

Pareiškėja prašė išsiaiškinti banko atsakomybę ir įsipareigojimus saugoti patekimą į pareiškėjos banko sąskaitą, taip pat įpareigoti banką grąžinti neteisėtu būdu trečiųjų asmenų iš jos banko sąskaitos nurašytus 1 000 Eur.

Bankas pateiktame atsiliepime Lietuvos bankui paaiškino mokėjimo operacijos inicijavimo ir įvykdymo aplinkybes ir informavo, kad 2020 m. rugsėjo 7 d. 22:41:25 val. pareiškėjos vardu atidarytoje banko sąskaitoje buvo duotas sutikimas įvykdyti 1 000 Eur mokėjimo operaciją gavėjui A DOBRE. Gavėjo sąskaita buvo atidaryta bendrovėje UAB „Trustcom Financial“ (Lietuvoje veikianti el. pinigų įstaiga), o mokėjimas įvykdytas kaip momentinis mokėjimas; 22:40:28 val. buvo vienas nesėkmingas bandymas prisijungti prie pareiškėjos interneto banko (jungėsi tretieji asmenys), nes buvo neteisingai suvestas pareiškėjos asmens kodas. Po 17 sekundžių 22:40:45 val. buvo sėkmingai prisijungta prie pareiškėjos interneto banko. Bankas pateiktame atsiliepime išdėstė turimus duomenis apie prisijungimo prie pareiškėjos interneto banko paskyros eiliškumą: banko adresu buvo pasirinka „SmartID“ kaip tapatybės patvirtinimo priemonė ir suvestas banko ID bei pareiškėjos asmens kodas, nes prie pareiškėjos interneto banko buvo jungiamasi iš banko dar nefiksuoto kaip klientės naudojamo galinio įrenginio. Šie veiksmai pareiškėjos telefone inicijavo „SmartID“ programėlės atidarymą. Programėlės „SmartID“ ekrane buvo rodomas kontrolinis kodas, kurį pareiškėja, prieš vesdama PIN1 ir taip duodama sutikimą prisijungti prie interneto banko, turėjo sutikrinti su interneto banko prisijungimo ekrane rodomu kontroliniu kodu. Pareiškėja suvedė PIN1 ir tokiu būdu davė sutikimą prisijungti prie savo interneto banko. Banko turimais duomenimis, pareiškėjos prisijungimo prie interneto banko sesija truko nuo 22:40:45 val. iki 22:41:16 val., t. y. 47 sekundes. Šios sesijos metu buvo suformuotas mokėjimo nurodymas, todėl buvo inicijuotas programėlės „SmartID“ ekrano atidarymas pareiškėjos telefone. Programėlės „SmartID“ ekrane pareiškėjai buvo rodomas kontrolinis kodas, kurį pareiškėja prieš vesdama PIN2 turėjo sulyginti su interneto banko aplinkoje rodomu kontroliniu kodu (jie turi sutapti). Bankas pažymėjo, kad, jeigu pareiškėja prieš vesdama PIN1 bei PIN2 būtų sulyginusi „SmartID“ programėlėje rodomus kontrolinius kodus su interneto banko aplinkoje rodomais kontroliniais kodais, pareiškėja būtų pastebėjusi, kad sukčių suklastotoje interneto banko aplinkoje, į kurią pareiškėja buvo patekusi paspaudusi SMS žinute gautą nuorodą, kontroliniai kodai neturėjo būti rodomi. Kontroliniai kodai buvo rodomi tikroje interneto banko aplinkoje, kurią ir matė sukčiai. Todėl, banko teigimu, vien ši aplinkybė pareiškėjai turėjo sukelti įtarimą ir sulaikyti pareiškėją nuo tolimesnių veiksmų.

Bankas taip pat pažymėjo, kad prieš pareiškėjai vedant PIN2 „SmartID“ programėlėje 22:41:16 val. buvo rodomi ne tik kontroliniai kodai, tačiau ir informacija, susijusi su mokėjimo pavedimu – suma, bei gavėjas. Banko turimais duomenimis, pareiškėja PIN2 kodą suvedė 22:41:25 val., t. y. per 9 sekundes nuo prašymo jį suvesti „SmartID“ programėlės lange pateikimo. Tačiau pareiškėja dėl savo didelio neatsargumo prieš vesdama PIN2 nekreipė dėmesio į rodomą informaciją, kad yra tvirtinamas 1 000 Eur mokėjimo pavedimas gavėjui A DOBRE. 22:41:27 val. bankas pareiškėjos programėlėje parodė pranešimą, kad yra įvykdytas 1 000 Eur mokėjimas gavėjui A DOBRE.

Pasisakydamas dėl pareiškėjos argumentų, kad neužtikrino jos piniginių lėšų saugumo, esančių banko sąskaitoje, bankas paaiškino, kad nesutinka su pareiškėjos nurodytais argumentais, ir teigė, kad pareiškėja lėšas prarado ne dėl banko kaltės, o dėl savo didelio neatsargumo. Teigdamas, kad pati pareiškėja, o ne bankas, yra atsakinga už tai, kad dėl mokėjimo operacijos, kuriai nedavė sutikimo, patyrė nuostolį, bankas remiasi Lietuvos Respublikos mokėjimų įstatymo 39 straipsnio 3 dalimi, kuri reglamentuoja, 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. Bankas teigia, kad pareiškėjos elgesys buvo labai neatsargus ir būtent šis pareiškėjos labai neatsargus elgesys lėmė nuostolio atsiradimą.

Bankas pažymėjo, kad pareiškėjos telefonu gauta neva banko siųsta SMS žinutė pareiškėjai turėjo sukelti įtarimų, nes SMS žinutė pareiškėjai buvo siųsta iš telefono numerio, kuris nėra niekaip siejamas nei su banku, nei su „SmartID“ programėle. Taip pat bankas ir anksčiau pareiškėjai niekada nesiųsdavo jokios informacijos SMS žinutėmis. Todėl vien ši aplinkybė pareiškėjai turėjo sukelti įtarimą, tačiau pareiškėja net nebandė įsitikinti, ar gauta SMS žinutė yra tikrai iš banko, todėl, banko nuomone, toks pareiškėjos elgesys gali būti

vertinamas kaip labai neatsargus.

Banko teigimu, pareiškėjos didelį neatsargumą rodo ir tai, kad, gavusi aktyvią nuorodą, ją paspaudė net nepatikrinusi, ar rodomas interneto banko adresas sutampa su tikruoju banko interneto banko adresu. Bankas teigia, kad mokėtojas turi pareigą, nustatytą Mokėjimų įstatymo 34 straipsnyje, įsitikinti, kad prie interneto banko jungiamasi tinkamu adresu, o adresą naršyklėje yra būtina surinkti pačiam vartotojui, o ne naudotis atsiųstomis nuorodomis. Jeigu pareiškėja būtų buvusi atidi ir būtų tikrinusi interneto banko adresą, ji būtų pastebėjusi, kad sukčių suklastotas interneto banko adresas skiriasi nuo tikrojo banko adreso, todėl būtų susilaikiusi nuo banko ID bei savo asmens kodo vedimo į sukčių suklastotą banko aplinką. Bankas pažymėjo, kad tiek viešojoje erdvėje, tiek ir banko klientams siunčiamuose įspėjimuose klientų dėmesys yra atkreipiamas į tai, kad reikia saugotis trečiųjų asmenų nusikalstamos veikos, todėl pareiškėja turėjo būti budri.

Bankas taip pat pažymėjo, kad pareiškėja turėjo pareigą laikytis banko ir pareiškėjos sudarytoje sutartyje bei Mokėjimų įstatymo 34 straipsnyje nustatytų pareigų. Banko teigimu, pareiškėja, prieš vesdama PIN2 ir taip duodama sutikimą įvykdyti mokėjimo operaciją, savo telefone esančioje programėlėje „SmartID" turėjo galimybę matyti kontrolinį kodą, kurį turėjo pareigą sulyginti su interneto banke rodomu kontroliniu kodu (jie turėjo sutapti). Vien tik aplinkybė, kad pareiškėja „SmartID" programėlėje rodomo kontrolinio kodo neturėjo su kuo sulyginti, turėjo pareiškėjai sukelti įtarimą, o pareiškėja turėjo susilaikyti nuo PIN2 kodo vedimo. Bankas nurodė, kad pareiga tikrinti kontrolinius kodus prieš vedant PIN kodus yra įtvirtinta „SmartID" atmintinėje, kuri yra skelbiama viešai banko puslapyje ir kuri yra neatskiriama pareiškėjos ir banko sutarties dalis.

Bankas taip pat nurodė, kad prieš vedant PIN2 „SmartID" programėlėje pareiškėjai buvo rodomi ne tik kontroliniai kodai, tačiau ir informacija, susijusi su mokėjimo pavedimu – suma, bei gavėjas. Banko teigimu, tai, kad pareiškėja nurodo, kad bankas jai informacijos su mokėjimo pavedimu nerodė, nereiškia, kad bankas tikrai minėtos informacijos „SmartID" programėlėje nerodė, nes banko sistemų turimi išrašai patvirtina, kad pareiškėjai su mokėjimo pavedimu susijusi informacija prieš vedant PIN2 buvo rodoma. Aplinkybė, kad pareiškėja netikrino ne tik kontrolinių kodų, bet ir prieš vesdama PIN2 nekreipė pakankamai dėmesio į tai, kad vesdama PIN2 tvirtina 1 000 Eur mokėjimo pavedimą gavėjui A DOBRE, rodo pareiškėjos didelį neatsargumą.

Bankas pažymėjo, kad užtikrina klientų lėšų sąskaitose saugumą ir kad prie klientų sąskaitų būtų galima prisijungti tik per banko interneto svetainę. Bankas paaiškino, kad pareiškėjai gavus SMS žinutę su aktyvia nuoroda ir ją paspaudus buvo atidaryta sukčių suklastota interneto banko aplinka, kuri tik vizualiai buvo panaši į tikrąją banko aplinką. Pareiškėjai šioje sukčių suklastotoje interneto banko aplinkoje suvedus banko ID ir savo asmens kodą, šiuos duomenis pasisavino sukčiai ir mokėjimo operaciją inicijavo prisijungę prie tikros pareiškėjos interneto banko aplinkos. Sukčiai inicijavo ir „SmartID" programėles atidarymą pareiškėjos telefone. Banko teigimu, pareiškėja dėl savo didelio neatsargumo į sukčių suklastotą interneto banko aplinką suvedė banko ID ir savo asmens kodą, todėl dėl didelio neatsargumo neišsaugojo ir sukčiams atskleidė savo tapatybės patvirtinimo priemones. Bankas paaiškino, kad banko klientams teikiamų saugaus naudojimosi el. paslaugomis rekomendacijų laikymasis turėjo pareiškėją sulaikyti nuo mokėjimo operacijos patvirtinimo. Banko teigimu, pareiškėja su banko teikiamomis saugaus naudojimosi el. paslaugomis rekomendacijomis buvo supažindinta asmeniškai banko 2020 m. balandžio 2 d. siųsta elektronine žinute interneto banke. Informacija apie pareigą laikytis saugaus naudojimosi el. paslaugomis rekomendacijų yra nurodyta ir Banko mokėjimo paslaugų teikimo sąlygų 7.1 papunktyje. Bankas nurodė, kad saugaus naudojimosi el. paslaugomis rekomendacijos yra skelbiamos viešai banko puslapyje bei prisijungiant prie interneto banko puslapio.

Bankas pažymėjo, kad visos pirmiau išdėstytos aplinkybės pagrindžia pareiškėjos didelį neatsargumą duodant sutikimą įvykdyti 1 000 Eur mokėjimo operaciją gavėjui A DOBRE. Bankas nurodo, kad didelis neatsargumas pasireiškia paprastų, visiems suprantamų elgesio taisyklių nesilaikymu arba asmeniui neabejotinai žinomų saugaus elgesio reikalavimų ignoravimu, kai asmuo turėjo ir galėjo numatyti žalos atsiradimą. Pareiškėja turėjo suprasti, kad „SmartID" yra prisijungimo prie jai teikiamos interneto banko aplinkos priemonė, kuri apsaugo patekimą prie pareiškėjos lėšų banko sąskaitoje. Todėl, banko teigimu, naudojantis „SmartID" yra būtina laikytis jos naudojimą reglamentuojančių sąlygų, kurios yra skelbiamos viešai banko puslapyje („SmartID" atmintinė). Taip pat kontroliniai

kodai yra viena iš svarbių saugumo priemonių, kuri užtikrina, kad mokėtojas būtų informuotas apie mokėjimo operacijos sumą ir gavėją, todėl pareiškėja negalėjo ignoruoti aplinkybės, kad ji neturėjo su kuo sulyginti „SmartID" programėlėje rodomų kontrolinių kodų. Bankas teigia, kad pareiškėja pažeidė „SmartID" naudojimo sąlygas, nesilaikė saugaus naudojimosi el. paslaugomis rekomendacijų ir dėl savo didelio neatsargumo davė sutikimą įvykdyti 1 000 Eur mokėjimą gavėjui A DOBRE. Todėl visi nuostoliai dėl neautorizuotos mokėjimo operacijos turi tekti pačiai pareiškėjai, bet ne bankui.

Atsižvelgdamas į pirmiau nurodytas aplinkybes, bankas prašė pareiškėjos reikalavimą grąžinti 1 000 Eur atmesti kaip nepagrįstą.

K o n s t a t u o j a m a:

Vadovaujantis Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių, patvirtintų Lietuvos banko valdybos 2012 m. sausio 26 d. nutarimu Nr. 03-23, 45 punktu, vartojimo ginčai Lietuvos banke nagrinėjami laikantis rungimosi, ginčų nagrinėjimo operatyvumo, koncentracijos, ekonomiškumo ir bendradarbiavimo principų. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą ir jo pagrindu priimamas sprendimas.

Pareiškėjos ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjai 2020 m. rugsėjo 7 d. pareiškėjos banko sąskaitoje atliktos 1 000 Eur mokėjimo operacijos (toliau – ginčijama mokėjimo operacija) sumą. Pareiškėja teigia, kad ginčijama mokėjimo operacija įvykdyta be pareiškėjos sutikimo, todėl bankas turi grąžinti pareiškėjai šios operacijos sumą. Bankas teigia, kad ginčijamos mokėjimo operacijos įvykdymą ir dėl to atsiradusį 1 000 Eur nuostolį lėmė tai, kad pareiškėja dėl didelio neatsargumo neįvykdė Mokėjimų įstatymo 34 straipsnyje bei sutartyje su banku nustatytų pareigų. Bankas savo sprendimą negrąžinti ginčijamos mokėjimo operacijos sumos grindžia Mokėjimų įstatymo 39 straipsnio 3 dalies nuostata, kuri reglamentuoja mokėtojo atsakomybę už neautorizuotas mokėjimo operacijas, kai nuostoliai patirti dėl mokėtojo didelio neatsargumo.

Nagrinėjamo ginčo atveju tarp šalių nėra ginčo, ar ginčijama mokėjimo operacija laikytina autorizuota, t. y. abi ginčo šalys sutinka, kad ginčijamai mokėjimo operacijai atlikti nebuvo duotas pareiškėjos sutikimas. Vadinasi, nagrinėjamo ginčo atveju ginčijama mokėjimo operacija laikytina neautorizuota. Atsižvelgiant į tai, Mokėjimų įstatymo nuostatos, susijusios su mokėjimo operacijos autorizavimu, toliau sprendime nebus aptariamos.

Siekiant išspręsti tarp pareiškėjos ir banko kilusį ginčą, Lietuvos banko vertinimu, būtina nustatyti, ar bankas turėjo (turi) pareigą grąžinti pareiškėjai ginčijamos neautorizuotos mokėjimo operacijos sumą.

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 Mokėjimų įstatymas (redakcija, galiojusi nuo 2019 m. spalio 20 d. iki 2020 m. spalio 1 d.).

Dėl neautorizuotos mokėjimo operacijos pasekmių ir pareiškėjos teisės į ginčijamos mokėjimo operacijos sumos grąžinimą

Mokėjimų įstatymo 36 straipsnio 1 dalyje nustatyta mokėtojo mokėjimo paslaugų teikėjo pareiga grąžinti mokėtojui neautorizuotos mokėjimo operacijos sumą, jeigu mokėtojas, sužinojęs apie neautorizuotas operacijas, apie tai praneša savo mokėjimo paslaugų teikėjui nedelsdamas, ne vėliau kaip per 13 mėnesių nuo lėšų nurašymo datos. Vadovaujantis Mokėjimų įstatymo 38 straipsnio 1 dalimi, neautorizuota mokėjimo operacija turi būti grąžinta mokėtojui nedelsiant, bet ne vėliau kaip iki kitos darbo dienos pabaigos, po to, kai mokėjimo paslaugų teikėjas sužino apie neautorizuotą mokėjimo operaciją.

Mokėjimų įstatymo 37 straipsnio 1 dalyje nustatyta, kad jeigu mokėtojas neigia autorizavęs įvykdytą mokėjimo operaciją ar teigia, kad mokėjimo operacija buvo įvykdyta netinkamai, jo mokėjimo paslaugų teikėjas turi įrodyti, kad mokėjimo operacijos autentiškumas buvo patvirtintas, ji buvo tinkamai užregistruota, įrašyta į sąskaitas ir jos nepaveikė techniniai trikdžiai arba kiti mokėjimo paslaugų teikėjo teikiamos paslaugos trūkumai; kai mokėtojas neigia autorizavęs įvykdytą mokėjimo operaciją, mokėtojo mokėjimo paslaugų teikėjo arba atitinkamais atvejais mokėjimo inicijavimo paslaugos teikėjo užregistruotas mokėjimo priemonės naudojimas nebūtinai yra pakankamas įrodymas, kad

mokėtojas autorizavo mokėjimo operaciją ar veikė nesąžiningai arba tyčia ar dėl didelio neatsargumo neįvykdė vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų. 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).

Mokėjimų įstatymo 39 straipsnio 2 dalyje nustatyta, kad mokėtojas dėl neautorizuotos mokėjimo operacijos 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 vykdymas, 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.

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 įrodomas mokėtojo sukčiavimas (nesąžiningumas arba tyčia) arba didelis neatsargumas (Mokėjimų įstatymo 37 straipsnio 3 dalis ir 39 straipsnio 3 dalis).

Remiantis pareiškėjos ir banko pateikta informacija, apie tai, kad pareiškėja neigia autorizavusi (davusi sutikimą) ginčijamą mokėjimo operaciją, bankas buvo informuotas tą pačią dieną, kai tik buvo įvykdyta ginčijama mokėjimo operacija, t. y. 2020 m. rugsėjo 7 d., ir tą pačią dieną bankas užblokavo pareiškėjos interneto banko paslaugą. Pareiškėja į banką dėl ginčijamos mokėjimo operacijos atšaukimo kreipėsi 2020 m. rugsėjo 8 d., o bankas tą pačią dieną kreipėsi į gavėjo banką dėl ginčijamos mokėjimo operacijos atšaukimo. Tačiau iš gavėjo banko bankas gavo informaciją, kad ginčijamos mokėjimo operacijos lėšos buvo iš karto įskaitytos į gavėjo sąskaitą ir iš karto pervestos kitiems asmenims į kitus bankus užsienio valstybėje. Nepaisant to, kad bankas galimybės atšaukti įvykdytos ginčijamos mokėjimo operacijos nebeturėjo, apie tai, kad pareiškėja neigia autorizavusi ginčijamą mokėjimo operaciją, bankui tapo žinoma nuo pareiškėjos kreipimosi į banką dienos.

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); nuostoliai yra patirti dėl mokėjimo paslaugų teikėjo, jo darbuotojo, tarpininko, filialo ar asmenų, kuriems perduotas veiklos funkcijų valdymas, veiksmų ar neveikimo (2 punktas).

Pagal Mokėjimų įstatymo 2 straipsnio 32 dalį, mokėjimo priemonė – personalizuota priemonė ir (arba) tam tikros procedūros, dėl kurių susitaria mokėjimo paslaugų vartotojas ir mokėjimo paslaugų teikėjas ir kurias mokėjimo paslaugų vartotojas naudoja mokėjimo nurodymui inicijuoti. Pasisavinimas šiuo atveju turėtų būti suprantamas kaip svetimos mokėjimo priemonės užvaldymas ir galėjimas ja naudotis kaip sava. Neteisėtumas suponuoja atlikto veiksmo teisinio pagrindo nebuvimą.

Nagrinėjamo ginčo byloje buvo nustatyta, kad 2020 m. rugsėjo 7 d. 22:14 val. pareiškėja į savo mobilųjį telefoną gavo SMS žinutę, kurioje buvo prašoma atnaujinti „SmartID" paskyrą, ir pagal žinutėje pateiktą nuorodą prisijungė prie interneto banko paskyros, kuri, kaip vėliau paaiškėjo, buvo suklastota (toliau – suklastota interneto banko paskyra). Pareiškėjai siųsta SMS žinutė buvo siųsta iš telefono numerio, kuriuo nei bankas, nei „SmartID" programėlės atstovai pareiškėjai anksčiau niekada nebuvo siuntę jokios SMS žinutės. Šią aplinkybę Lietuvos bankui patvirtino ir pati pareiškėja. Pareiškėjos teigimu, prie suklastotos interneto banko paskyros ji prisijungė tikėdamasi, kad atnaujina „SmartID" paskyrą, kaip tai buvo nurodyta pareiškėjos gautoje SMS žinutėje, ir suklastotoje interneto banko paskyroje suvedė savo asmens kodą, banko ID, o „SmartID" programėlėje PIN kodus turėdama tikslą atnaujinti „SmartID". Banko pateiktais duomenimis, pareiškėjai sukčių suklastotoje interneto banko aplinkoje suvedus banko ID bei savo asmens kodą, sukčiai šiuos duomenis nusavino ir 22:40:28 val. jungėsi prie tikrosios pareiškėjos interneto banko aplinkos. Remiantis pareiškėjos ir banko pateiktais duomenimis, darytina išvada, kad 2020 m. rugsėjo 7 d. 22:40:28 val. prie interneto banko jungėsi ne pati pareiškėja, o tretieji asmenys,

kurie, nukreipdami pareiškėją į suklastotą banko interneto banko paskyrą, neteisėtai išviliojo ir pasisavino prisijungti prie interneto banko sistemos reikalingus duomenis ir juos panaudojo tos pačios dienos prisijungimui prie pareiškėjos interneto banko paskyros ir joje inicijavo ginčijamą mokėjimo operaciją.

Įvertinus pareiškėjos ir banko pateiktą informaciją apie trečiųjų asmenų neteisėtus veiksmus, dėl kurių iš pareiškėjos banko sąskaitos, nesant pareiškėjos sutikimo, buvo įvykdyta ginčijama mokėjimo operacija, galima pagrįstai daryti išvadą, kad atliekant ginčijamą mokėjimo operaciją banko pareiškėjai išduota mokėjimo priemonė ir jos personalizuoti saugumo duomenys buvo neteisėtai pasisavinti

Bankas teigia, kad pareiškėja galėjo išvengti neteisėto mokėjimo priemonės ir jos personalizuotų saugos duomenų pasisavinimo, jeigu tik būtų buvusi pakankamai atidi, o sukčiai pareiškėjos mokėjimo priemonę ir jos personalizuotus saugos duomenis pasisavino tik dėl to, kad pareiškėjos elgesys, gavus sukčių SMS žinutę su nuoroda, paspaudus nurodą ir sukčių suklastotoje interneto banko aplinkoje suvedus banko ID bei asmens kodą, buvo labai neatsargus.

Vertinant tai, ar pareiškėja galėjo pastebėti mokėjimo priemonės praradimą iki ginčijamos mokėjimo operacijos įvykdymo, būtina atsižvelgti, be kita ko, į tai, kad: 1) pareiškėja sukčių SMS žinutę gavo iš telefono numerio, kuris nebuvo susietas su banko telefono numeriu; 2) atidariusi aktyvią nuorodą, pareiškėja pateko į suklastotą interneto banko paskyrą, kuri jai objektyviai galėjo atrodyti kaip tikra interneto banko aplinka; 3) personalizuotus saugumo duomenis pareiškėja atskleidė norėdama atnaujinti „SmartID" programėlę, o ne siekdama įvykdyti ginčijamą arba bet kurią kitą mokėjimo operaciją; 4) apie tai, kad suklastotoje interneto banko paskyroje įvesti personalizuoti saugumo duomenys tapo žinomi tretiesiems asmenims ir šie asmenys juos panaudojo ginčijamai mokėjimo operacijai atlikti, pareiškėjai, turimais ginčo bylos duomenimis, tuo metu nebuvo žinoma; apie šias aplinkybes pareiškėja sužinojo tik po to, kai gavo banko pranešimą, kad yra įvykdytas mokėjimo nurodymas; 5) sužinojusi, kad yra atlikta ginčijama mokėjimo operacija ir pasisavinti personalizuoti saugumo duomenys bei interneto bankas, pareiškėja nedelsdama kreipėsi į banką ir informavo jį apie tai, kad ginčijama mokėjimo operacija yra neautorizuota.

Šalių ginčo dėl to, kad pareiškėja galėjo veikti nesąžiningai arba tyčia, įskaitant sukčiavimą, nėra, todėl darytina išvada, kad bankas pripažįsta, kad pareiškėjos veiksmuose neįžvelgia nesąžiningumo ir (arba) tyčios, t. y. neįžvelgia pareiškėjos veiksmuose galimo sukčiavimo požymių. Lietuvos banko vertinimu, visos pirmiau minėtos aplinkybės nesudaro pagrindo teigti, kad pareiškėja galėjo pastebėti, jog mokėjimo priemonė galėjo būti sukčių pasisavinta. Banko atsiliepime nurodytos aplinkybės, kad pareiškėjos telefonu gauta neva banko siųsta SMS žinutė pareiškėjai turėjo sukelti įtarimų (kadangi SMS žinutė pareiškėjai buvo siųsta iš telefono numerio, kuris nėra niekaip siejamas su banku ar su „SmartID" programėle) ir pareiškėja turėjo susilaikyti nuo tolimesnių veiksmų, t. y. nespausti aktyvios nuorodos, taip pat banko atsiliepime nurodyta aplinkybė, kad pareiškėja turėjo pastebėti, kad paspaudusi aktyvią nuorodą pateko į sukčių suklastotą aplinką, nes skyrėsi banko adresas, Lietuvos banko nuomone, nesuteikia pagrindo vertinti, kad vidutiniškai atidus ir protingas vartotojas galėtų neabejotinai pastebėti ir suprasti, kad SMS žinutę gavo ne iš banko ir kad sukčių suklastota interneto banko aplinka, kuri vizualiai buvo panaši į tikrą banko aplinką, nėra tikroji banko aplinka. Pareiškėjai, kaip vidutiniškai protingai vartotojai, objektyviai galėjo atrodyti, kad ji pateko į banko interneto banko aplinką, kuri buvo vizualiai panaši į tikrą banko aplinką, ir kad banko ID bei asmens kodą veda į tikrą banko aplinką. Be to, pareiškėja Lietuvos bankui nurodė, kad tai, kad jos prašoma suvesti asmens kodą, jai nesukėlė jokių įtarimų, nes buvo susiklosčiusi tokia praktika, kad ir anksčiau bankas prašydavo jungiantis prie interneto banko papildomai suvesti ir asmens kodą.

Lietuvos banko nuomone, vertinant pareiškėjos elgesį pagal vidutinio vartotojo standartą, galima būtų teigti, kad pareiškėjos elgesys, atidarius SMS žinute gautą nuorodą bei vizualiai panašoje sukčių suklastotoje banko aplinkoje suvedus banko ID bei asmens kodą, galėtų būti vertinamas tik kaip neatsargus, tačiau šio konkretaus ginčo atveju negalėtų būti vertinamas kaip labai neatsargus elgesys.

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 arba 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 (2 dalis).

Siekiant įvertinti, ar nagrinėjamo ginčo byloje pareiškėjos atžvilgiu galėtų būti taikoma Mokėjimo įstatymo 39 straipsnio 3 dalis, būtina nustatyti, ar pareiškėjos elgesys, atidarant SMS žinute gautą nuorodą ir suklastotoje banko interneto banko paskyroje suvedant personalizuotus saugumo duomenis (banko ID ir asmens kodą), o „SmartID" programėlėje – PIN kodus, gali būti vertinamas kaip didelis pareiškėjos neatsargumas (aplaidumas), dėl kurio visi nuostoliai, susiję su ginčijamos mokėjimo operacijos įvykdymu, turėtų tekti pareiškėjai. Kaip ir minėta prieš tai, pačios pareiškėjos sukčiavimo (nesąžiningumas arba tyčia) aplinkybė nėra vertinama, nes ginčo byloje duomenų apie galimą pareiškėjos sukčiavimą nėra, o ginčo šalys galimo sukčiavimo aplinkybe nesiremia.

Didelio neatsargumo sąvoka plėtojama 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 (Lietuvos Aukščiausiojo Teismo 2017 m. balandžio 13 d. nutartis civilinėje byloje Nr. e3K-3-180-378/2017, 29 punktas)."

Kasacinis teismas civilinėje byloje (byla Nr. 3K-3-222-219/2017) pateikė išaiškinimą, kas galėtų būti laikoma dideliu neatsargumu teikiant mokėjimo paslaugas: „Teisėjų kolegija nurodo, kad ieškovas suprato arba turėjo suprasti, kad jam atsakovės suteikti slapti ir tik jam žinomi prisijungimo prie sąskaitų duomenys apsaugo jo sąskaitas. Jų atskleidimas tretiesiems asmenims, juo labiau neidentifikuotiems telefoniniu ryšiu, pažeidė sąskaitų apsaugą ir sudarė galimybę tretiesiems asmenims pasinaudoti sąskaitose esančiais pinigais, todėl personalizuotų (slaptų, žinomų tik vartotojui) prisijungimo prie sąskaitų duomenų atskleidimas telefoniniu ryšiu tretiesiems asmenims rodo ne tik ieškovo neteisėtus, pažeidžiančius sutarties sąlygas veiksmus (Mokėjimų įstatymo 25 straipsnis), bet ir neprotingą, išskirtinai nerūpestingą elgesį, kuris kvalifikuotinas kaip didelis neatsargumas, lėmęs pinigų iš jo sąskaitų pervedimą tretiesiems asmenims. Todėl jam tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai (Mokėjimų įstatymo 30 straipsnio 2 dalis)."

Bankas, siekdamas pagrįsti, kad pareiškėja, atidarydama SMS žinute gautą nuorodą ir suklastotoje interneto banko paskyroje suvesdama banko ID, savo asmens kodą, o „SmartID" programėlėje PIN1 bei PIN2, nebuvo pakankamai rūpestinga ir apdairi, be pirmiau paminėtų aplinkybių (SMS žinutės gavimo bei aktyvios nuorodos atidarymo), remiasi aplinkybėmis, kad: pareiškėja, prieš vesdama PIN1 ir PIN2 ir taip duodama sutikimą prisijungti prie interneto banko bei įvykdyti mokėjimo operaciją, savo telefone esančioje programėlėje „SmartID" turėjo galimybę matyti kontrolinius kodus, kuriuos turėjo pareigą sulyginti su interneto banke rodomais kontroliniais kodais (jie turėjo sutapti). Vien tik aplinkybė, kad pareiškėja „SmartID" programėlėje rodomų kontrolinių kodų neturėjo su kuo sulyginti, turėjo pareiškėjai sukelti įtarimą, o pareiškėja turėjo susilaikyti nuo PIN2 kodo vedimo; prieš vedant PIN2 „SmartID" programėlėje pareiškėjai buvo rodoma informacija, susijusi su mokėjimo pavedimu – suma, bei gavėjas. Aplinkybė, kad pareiškėja netikrino ne tik kontrolinių kodų, bet ir prieš vesdama PIN2 nekreipė pakankamai dėmesio į tai, kad vesdama PIN2 tvirtina 1 000 Eur mokėjimo pavedimą gavėjui A DOBRE, rodo pareiškėjos didelį neatsargumą; pareiškėja su banko teikiamomis saugaus naudojimosi el. paslaugomis rekomendacijomis buvo supažindinta asmeniškai banko siųsta 2020 m. balandžio 2 d. elektronine žinute interneto banke. Informacija apie pareigą laikytis saugaus naudojimosi el. paslaugomis rekomendacijų yra nurodyta ir Banko mokėjimo paslaugų teikimo sąlygose ir banko viešai skelbiama tinklalapyje.

Vertinant tai, ar pirmiau paminėtos aplinkybės galėtų sudaryti pagrindą pareiškėjos elgesį vertinti kaip didelį neatsargumą, Lietuvos banko nuomone, didelis neatsargumas turėtų būti objektyviai aiškus, t. y. pasireikšti esminiu pareigos elgtis rūpestingai pažeidimu ir (arba) atsargumo priemonių nepaisymu, asmens galėjimu numatyti tokio nerūpestingo elgesio pasekmes bei veiksmų išvengti tokių pasekmių nesiėmimu. 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."

Vertinant tai, ar pareiškėjos elgesys pasireiškė esminiu pareigos elgtis rūpestingai pažeidimu ir (arba) atsargumo priemonių nepaisymu bei pareiškėjos galėjimu numatyti tokio nerūpestingo elgesio pasekmes bei imtis veiksmų, kad jų būtų išvengta, Lietuvos banko vertinimu, ne visos banko nurodomos kaip įrodančios pareiškėjos didelį neatsargumą aplinkybės suteiktų pagrindą teigti, kad pareiškėjos veiksmai galėjo turėti didelio neatsargumo požymių. Kaip jau buvo konstatuota pirmiau, Lietuvos banko vertinimu, pareiškėjos elgesys, atidarius SMS žinute gautą nuorodą bei vizualiai panašoje sukčių suklastotoje banko aplinkoje suvedus banko ID bei asmens kodą ir tokiu būdu juos atskleidus tretiesiems asmenims, nevertintinas kaip labai neatsargus (aplaidus) elgesys, o tik kaip neatsargus.

Bankas taip pat teigia, kad pareiškėja, prieš vesdama tiek PIN1, tiek PIN2 ir taip duodama sutikimą prisijungti prie interneto banko bei įvykdyti mokėjimo operaciją, savo telefone esančioje programėlėje „SmartID" turėjo galimybę matyti kontrolinius kodus ir juos privalėjo sulyginti su interneto banke rodomais kontroliniais kodais (jie turėjo sutapti), tačiau pareiškėja šios pareigos nevykdė, todėl pažeidė Mokėjimų įstatymo 34 straipsnio ir sutarties su banku nuostatas. Bankas teigia, kad pareiga tikrinti kontrolinius kodus prieš vedant PIN kodus yra įtvirtinta „SmartID" atmintinėje, kuri yra skelbiama viešai banko puslapyje ir kuri yra neatskiriama pareiškėjos ir banko sudarytos sutarties dalis. Bankas Lietuvos bankui pateikė įrodymus, kurie patvirtina, kad tiek „SmartID" programėlėje, tiek banko interneto banko paskyroje prieš vedant PIN kodus pareiškėjai buvo rodomi kontroliniai kodai. Pareiškėja Lietuvos bankui paaiškino, kad minėtų kontrolinių kodų netikrino, nes manė, kad atnaujina „SmartID" programėlę, o ne tvirtina mokėjimo operaciją. Taigi, pareiškėja neginčija mačiusi „SmartID" programėlėje rodomus kontrolinius kodus, tačiau jų nesutikrinusi su interneto banko aplinkoje rodomais kontroliniais kodais.

Vertinant, ar pareiškėja nesutikrindama kontrolinių kodų pažeidė sutarties su banku nuostatas, svarbu atkreipti dėmesį, kad banko nurodoma pareiga tikrinti kontrolinius kodus prieš vedant PIN kodus yra nustatyta banko viešai skelbiamoje „SmartID" atmintinėje: „Neskubėkite – patikrinkite kontrolinį kodą ir neveskite PIN kodų, jei neatliekate jokios operacijos. Prieš įvesdami „Smart-ID" PIN1 arba PIN2 kodą, žvilgtelėkite į virš jų rodomą kontrolinį kodą ir sulyginkite jį su rodomu interneto banko ar programėlės lange." Banko teigimu, ši atmintinė yra sudedamoji sutarties, sudarytos tarp banko ir pareiškėjos, dalis.

Vertinant, ar banko tinklalapyje viešai skelbiama „SmartID" atmintinė gali būti laikoma sudėtine banko ir pareiškėjos sudarytos sutarties dalimi, svarbu įvertinti minėtos sutarties nuostatas, apibrėžiančias sutarties šalių teisinių santykių reguliavimą.

Banko Lietuvos bankui pateiktos banko ir pareiškėjos 2006 m. balandžio 10 d. sudarytos Elektroninių paslaugų teikimo sutarties (toliau – Sutartis) 2.3 papunktyje nustatyta, kad „šios sutarties reglamentuojamus santykius taip pat reglamentuoja Lietuvos Respublikos civilinis kodeksas, kiti įstatymai ir teisės aktai, Banko klientų aptarnavimo ir paslaugų teikimo bendrosios sąlygos bei operacijų atlikimą reglamentuojantys banko vidaus aktai, su kuriais klientas gali susipažinti sutartyje numatytu būdu arba kitu banko nurodytu būdu". Banko elektroninių paslaugų teikimo sąlygų 2.3 papunktyje nustatyta, kad „sutarties reglamentuojamus santykius taip pat reglamentuoja Lietuvos Respublikos civilinis kodeksas, kiti įstatymai ir teisės aktai, Bendrosios sąlygos, Mokėjimo sąlygos bei *Operacijų atlikimą reglamentuojantys kiti viešai Banko paskelbti dokumentai*, *su kuriomis Naudotojas gali susipažinti Banko tinklalapyje bei Banko padaliniuose*". Banko klientų aptarnavimo ir paslaugų teikimo bendrųjų sąlygų 2.1.6 papunktyje nurodyta, kad „sutarties sudėtine dalimi gali būti atitinkamos Paslaugos standartinės sąlygos, kurios yra skelbiamos Banko tinklalapyje internete. Klientas sudarydamas Sutartį ar jos pakeitimą susipažįsta su tokiomis sąlygomis Banko tinklalapyje internete arba, jam pageidaujant, Banko klientų aptarnavimo padalinyje, ir tokios Paslaugos standartinės sąlygos nėra pasirašomos, spausdinamos ar pridedamos prie Sutarties, tačiau jos yra laikomos neatskiriama Sutarties dalimi. Klientui ir Bankui susitarus, su konkrečios Sutarties sąlygomis Klientas gali susipažinti naudodamasis Elektroninėmis mokėjimo priemonėmis." Įvertinus pirmiau minėtas banko paslaugų teikimo sąlygų nuostatas,

kad banko ir pareiškėjos santykius gali reglamentuoti ir banko tinklalapyje viešai skelbiami dokumentai, galima teigti, kad „SmartID" atmintinė galėtų būti laikoma sudėtine Sutarties dalimi. Svarbu pažymėti, kad, banko pateiktais duomenimis, bankas pareiškėjai elektronine žinute interneto banke 2019 m. gegužės 30 d. siuntė informaciją apie atnaujintas Elektroninių paslaugų teikimo sąlygas, o pareiškėja banko siųstą žinutę perskaitė. Vis dėlto atkreiptinas dėmesys į tai, kad banko nurodoma mokėtojo pareiga tikrinti kontrolinius kodus prieš vedant PIN kodus nėra nustatyta jokiose kitose banko paslaugų teikimo sąlygose.

Lietuvos banko vertinimu, „SmartID" atmintinėje banko pateikiama informacija apie kontrolinius kodus (ją bankas nurodo kaip pareigos nustatymą) nesudaro pagrindo daryti išvadą, kad bankas pareiškėjai buvo nustatęs pareigą prieš „SmartID" programėlėje vedant PIN kodus sutikrinti ir kontrolinius kodus (rodomus „SmartID" programėlėje ir interneto banko paskyroje). „SmartID" atmintinėje pateikiama informacija apie kontrolinių kodų tikrinimą yra daugiau informacinio pobūdžio, joje nėra formuluojama (nustatoma) mokėtojo pareiga prieš vedant PIN kodus sutikrinti ir kontrolinius kodus, todėl labiau galėtų būti vertinama kaip rekomendacija, bet ne kaip vidutiniam vartotojui aiškiai suprantamos pareigos tikrinti kontrolinius kodus nustatymas. Taip pat, kaip ir buvo minėta, mokėtojo pareiga tikrinti kontrolinius kodus niekaip nėra apibrėžta ir Sutartyje bei jos kitose sudedamosiose dalyse. Be to, atkreiptinas dėmesys, kad „SmartID" atmintinė, pateikiama banko interneto banko tinklalapyje, nėra aiškiai matoma (pateikiama tik nuoroda į ją, kuri nėra aiškiai matoma (pastebima), todėl vidutinis vartotojas vien tik atdaręs banko tinklalapį šios informacijos gali nepastebėti. Bankas Lietuvos bankui nurodė, kad programėlės kūrėjai viešai teikia informaciją apie būtinybę kiekvieną kartą sulyginti rodomą kontrolinį kodą prieš suvedant PIN kodus. Tačiau ginčo byloje Lietuvos bankui nėra pateiktų duomenų, kad pareiškėja su šia informacija būtų buvusi supažindinta.

Atsižvelgiant į tai, kad „SmartID" atmintinėje pateikiama informacija mokėtojams prieš vedant PIN kodus sutikrinti ir kontrolinius kodus, Lietuvos banko nuomone, negali būti vertinama kaip tokios pareigos vartotojui (mokėtojui) nustatymas, ir į tai, kad pati „SmartID" atmintinė nėra vartotojams pateikiama aiškiai matomoje vietoje, kad šie galėtų su tokia informacija susipažinti, negalima pritarti banko nuomonei, kad pareiškėja netikrindama kontrolinių kodų pažeidė su banku sudarytos Sutarties nuostatas.

Turimais duomenimis, pareiškėja buvo aktyvi „SmartID" programėlės naudotoja (nuo 2020 m. sausio 1 d. iki 2020 m. rugsėjo 7 d. buvo prisijungusi ne mažiau kaip 158 kartus), todėl negalima teigti, kad pareiškėja su kontroliniais kodais, rodomais „SmartID" ir interneto banko paskyroje, nebuvo susidūrusi anksčiau. Pareiškėja ir telefonu Lietuvos bankui patvirtino, kad kontrolinius kodus matė, tačiau jų nesutikrino, nes manė, kad atnaujina „SmartID" programėlę. Vadinasi, pareiškėjai buvo suprantama kontrolinių kodų paskirtis. Jeigu pareiškėja būtų tikrinusi kontrolinį kodą prieš vesdama PIN1 ir taip duodama sutikimą prisijungti prie interneto banko paskyros, jau tada būtų pastebėjusi, kad neturi su kuo sulyginti „SmartID" programėlėje matomo kontrolinio kodo, ir, tikėtina, būtų susilaikiusi nuo tolimesnių veiksmų ir nesudariusi galimybės tretiesiems asmenims prisijungti prie tikrosios pareiškėjos interneto banko paskyros bei suformuoti mokėjimo pavedimo. Lietuvos banko turimais duomenimis, pareiškėjai kontroliniai kodai buvo rodomi ir prieš vedant PIN2 ir taip duodant sutikimą įvykdyti mokėjimo operaciją. Pareiškėja ir antrą kartą prieš vesdama PIN2 kontrolinių kodų netikrino, tačiau, jeigu būtų tikrinusi, tikėtina, būtų išvengusi mokėjimo operacijos patvirtinimo.

Vis dėlto, atsižvelgiant į tai, kad bankas nebuvo aiškiai pareiškėjai suformavęs pareigos prieš vedant PIN kodus sutikrinti ir kontrolinius kodus, pareiškėjos elgesys – PIN kodus suvedė nesutikrinusi kontrolinių kodų, galėtų būti vertinamas kaip neatsargus, bet ne kaip labai neatsargus (aplaidus) elgesys, pažeidžiantis Sutarties ar Mokėjimų įstatymo 34 straipsnio nuostatas.

Bankas taip pat teigia, kad prieš vedant PIN2 „SmartID" programėlėje pareiškėjai buvo rodomi ne tik kontroliniai kodai, tačiau ir informacija, susijusi su mokėjimo pavedimu – suma, bei gavėjas. Pareiškėja teigia, kad tokios informacijos nematė. Bankas Lietuvos bankui pateikė įrodymus (išrašus iš sistemos), kurie patvirtina, kad bankas prieš vedant PIN2 „SmartID" rodė ne tik kontrolinius kodus, bet ir mokėjimo pavedimo sumą bei gavėją. Svarbu pažymėti, kad telefono ekrano, kurį matė pareiškėja prieš vesdama PIN2, nuotrauka Lietuvos bankui nėra pateikta, tačiau, atlikus bandymą pasinaudojant banko „SmartID" programėle patvirtinti mokėjimo nurodymą, galima matyti, kad programėlės ekrane informacija apie mokėjimo operacijos sumą ir gavėją yra pateikiama aiškiai matomoje vietoje – iš karto po

kontroliniais kodais. Lietuvos banko nuomone, svarbu ne tik tai, kad bankas gali įrodyti, kad „SmartID" programėlėje rodė su mokėjimo pavedimu susijusią informaciją, tačiau ir tai, kaip aiškiai (matomai) ta informacija mokėtojui yra pateikiama. Nagrinėjamo ginčo atveju galima teigti, kad bankas su mokėjimo pavedimu susijusią informaciją rodė aiškiai, vidutiniam vartotojui aiškiai pastebimoje vietoje (iš karto po kontroliniu kodu, kuris yra pateiktas didesniu šriftu ir yra paryškintas). Lietuvos banko vertinimu, vidutiniškai atidžiam ir rūpestingam vartotojui tokiu būdu pateikiama informacija apie mokėjimo pavedimą ir jo duomenis turėjo ir galėjo būti matoma, todėl pareiškėja turėjo ir galėjo suprasti, kad vesdama PIN2 tvirtina mokėjimo pavedimą. Kaip minėta pirmiau, pareiškėja neneigia pastebėjusi „SmartID" programėlėje rodomus kontrolinius kodus, tačiau į juos neatkreipė pakankamo dėmesio. Banko pateiktais duomenimis, pareiškėja aktyviai naudojosi „SmartID" programėle, todėl turėjo ir galėjo suprasti, kad „SmartID" programėlėje PIN2 kodas yra naudojamas ir tvirtinant mokėjimo pavedimą. Be to, ir Mokėjimo paslaugų teikimo sąlygų 3.3.1 papunktyje nustatyta, kad sutikimas įvykdyti mokėjimo operaciją gali būti patvirtinamas elektroniniu parašu, klientui suteiktu slaptažodžiu, kodais ir (arba) kitomis tapatybės patvirtinimo priemonėmis.

Lietuvos banko vertinimu, atsižvelgiant į tai, kad banko pateikiama su mokėjimo pavedimu susijusi informacija (suma ir gavėjas) buvo rodoma aiškiai, pareiškėja prieš vesdama PIN2 turėjo ir galėjo pastebėti ir suprasti, kad vesdama PIN2 tvirtina mokėjimo nurodymą, tačiau pareiškėja banko rodomos su mokėjimo pavedimu susijusios informacijos nepastebėjo dėl elementarių atsargumo reikalavimų nesilaikymo. Jeigu pareiškėja prieš vesdama PIN2 kodą būtų bent atkreipusi dėmesį į „SmartID" programėlėje iš karto po kontroliniu kodu rodomą informaciją, ji būtų pastebėjusi, kad yra suformuotas 1 000 Eur mokėjimo pavedimas gavėjui A DOBRE, ir būtų susilaikiusi nuo PIN2 vedimo ir taip išvengusi lėšų iš savo banko sąskaitos praradimo. Pagal banko pateiktą informaciją, nuo momento, kai bankas parodė su mokėjimo pavedimu susijusią informaciją programėlės ekrane, iki momento, kai pareiškėja suvedė PIN2, praėjo 9 sekundės. Taigi, laiko tarpas, per kurį pareiškėja suvedė PIN2, buvo pakankamai ilgas, kad pareiškėja susipažintų su „SmartID" programėlės ekrane rodoma su mokėjimo pavedimu susijusia informacija.

Papildomai pažymėtina, kad, Lietuvos bankui pateiktais duomenimis, 2020 m. balandžio 2 d. pareiškėjai bankas elektronine žinute interneto banko paskyroje buvo siuntęs informaciją ir atkreipęs pareiškėjos dėmesį į galimas sukčių atakas. Pirmiau minėtoje banko pareiškėjai siųstoje žinutėje nurodoma, kad: „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 banko interneto svetaines". Taip pat žinutėje nurodoma – „prie banko junkitės tiesiogiai – patys suvedę mūsų svetainės adresą ar per programėlę. Nesijunkite per gautas nuorodas". Lietuvos banko turimais duomenimis, pareiškėja su šia banko žinute buvo susipažinusi.

Įvertinus ginčo byloje nustatytas aplinkybes – prieš vedant PIN2 kodą „SmartID" programėlėje buvo rodoma su mokėjimo operacija susijusi informacija (mokėjimo suma ir gavėjas), ji buvo rodoma aiškiai ir vidutiniškai atidžiam ir rūpestingam vartotojui pastebimoje vietoje, tačiau pareiškėja vesdama PIN2 į jai su mokėjimo operacija susijusią rodomą informaciją dėl savo didelio nerūpestingumo nekreipė dėmesio, darytina išvada, kad pareiškėjos elgesys laikytinas dideliu pareiškėjos neatsargumu (aplaidumu), lėmusiu tai, kad pareiškėjos pingines lėšas iš sąskaitos pasisavino tretieji asmenys. Kaip minėta, tiek Kasacinio teismo praktikoje, tiek PSD2 aiškiai pasisakoma, kad didelis neatsargumas turėtų pasireikšti labai dideliu aplaidumu. Nagrinėjamo ginčo atveju, jeigu pareiškėja nebūtų elgusis itin nerūpestingai (aplaidžiai) ir prieš vesdama PIN2 būtų atkreipusi dėmesį į aiškiai banko rodomą su mokėjimo pavedimu susijusią informaciją, pareiškėja nebūtų suvedusi PIN2 kodo ir 1 000 Eur mokėjimas nebūtų buvęs pateiktas vykdyti.

Kaip jau buvo minėta pirmiau, Lietuvos banko nuomone, pareiškėjos elgesys, kai ji atidarė nuorodą, gautą SMS žinute, ir vizualiai panašioje sukčių suklastotoje banko aplinkoje suvedė banko ID ir asmens kodą, o prieš vesdama PIN1 ir PIN2 nesutikrino rodomų kontrolinių kodų, galėtų būti vertinamas tik kaip neatsargus pareiškėjos elgesys.

Svarbu pažymėti, kad, nors ne visos nustatytos aplinkybės įvertintos kaip pareiškėjos didelis neatsargumas (aplaidumas), tačiau, vertinant nustatytų aplinkybių visumą, galima daryti išvadą, kad pareiškėjos nerūpestingas elgesys iki vedant PIN2 kodą galiausiai lėmė ir tai, kad pareiškėja dėl savo didelio neatsargumo vesdama PIN2 kodą nepastebėjo, kad šiuo veiksmu tvirtina mokėjimo pavedimą.

Įvertinus pirmiau išdėstytą informaciją, konstatuotina, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, todėl, Lietuvos banko vertinimu, bankas neturi pareigos pareiškėjai grąžinti neautorizuotos mokėjimo operacijos lėšų.

Dėl momentinių mokėjimų

Pareiškėja Lietuvos banko papildomai prašė paaiškinti, kodėl buvo pasirinktas ir įvykdytas momentinis mokėjimas ir per kiek laiko jis yra įvykdomas.

Prie pareiškėjos interneto banko paskyros nusavinę pareiškėjos banko ID ir asmens kodą, prisijungė tretieji asmenys ir iš pareiškėjos banko sąskaitos suformavo 1 000 Eur mokėjimą, kurį pasirinko kaip momentinį mokėjimą. Banko paslaugų ir operacijų įkainių sąlygose nustatyta, kad mokėjimas, kurio suma neviršija 15 000 Eur, vykdomas pagal Europos Sąjungoje veikiančios momentinių mokėjimų schemos taisykles. Tai reiškia, kad pirmenybė teikiama momentiniam mokėjimui. Svarbu pažymėti, kad pats mokėtojas gali aktyviais savo veiksmais interneto banke pasirinkti, ar mokėjimas bus atliekamas kaip momentinis, ar kaip įprastas, tačiau nagrinėjamo ginčo atveju momentinį mokėjimą inicijavo (pasirinko) tretieji asmenys, prisijungę prie pareiškėjos interneto banko paskyros. Pasirinkus momentinį mokėjimą, pinigai į gavėjo sąskaitą įskaitomi per kelias sekundes bet kuriuo paros metu, bet kurią metų dieną. Dėl šios priežasties, pareiškėjai kreipusis į banką dėl neautorizuotos mokėjimo operacijos, o vėliau ir dėl mokėjimo operacijos atšaukimo, momentinis mokėjimas jau buvo įvykdytas, t. y. pinigai jau buvo patekę į gavėjo sąskaitą, todėl bankas įvykdyto mokėjimo nebegalėjo atšaukti.

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

Atmesti pareiškėjos X.X. reikalavimą

Lietuvos banko sprendimas dėl ginčo esmės yra rekomendacinio pobūdžio ir teismui neskundžiamas. Vartotojui ir finansų rinkos dalyviui išlieka teisė dėl ginčo sprendimo kreiptis į teismą arba kitą ginčų nagrinėjimo instituciją įstatymų nustatyta tvarka. Kreipimasis į teismą po Lietuvos banko sprendimo dėl ginčo esmės priėmimo nelaikomas šio sprendimo apskundimu.

Direktorius Arūnas Raišutis