LIETUVOS BANKO
TEISĖS IR LICENCIJAVIMO DEPARTAMENTO
DIREKTORIUS

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

2022 m. birželio 13 d. Nr. 429-225
Vilnius

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

N u s t a t y t a:

2021 m. spalio 3 d. 18.52 val. pareiškėja į savo mobilųjį telefoną gavo trečiųjų asmenų siųstą tokio turinio SMS pranešimą: „Jusu SEB paskyra buvo itraukta i karantino zona, reikia is naujo patvirtinti. Uzkirsti kelia karantinui, jus turite atlikti siuos veiksmus cia: HK38721.com". Supratusi, kad yra įspėjama apie „Smart-ID" paskyros įtraukimą į karantino zoną ir informuojama apie būtinybę atnaujinti šią paskyrą paspaudžiant SMS pranešime pateiktą nuorodą, pareiškėja ją paspaudė ir atsidariusiame trečiųjų asmenų sukurtame interneto tinklalapyje suvedė savo interneto banko atpažinimo kodą (ID), asmens kodą ir, savo mobiliajame įrenginyje į savo „Smart-ID" paskyrą (toliau - Paskyra1) gavusi patvirtinimo kodus, suvedė Paskyros1 PIN1 ir PIN2 kodus.

2021 m. spalio 3 d. 20.22 val. tretieji asmenys savo įrenginyje pareiškėjos vardu sukūrė „Smart-ID Basic" paskyrą (toliau – Paskyra2) ir ja naudodamiesi pareiškėjos vardu aktyvino banko mobiliąją programėlę, prie kurios prisijungę 20 val. 37 min. 40 sek. atliko 5 150 Eur kredito pervedimą (toliau – Ginčijamas mokėjimas).

2021 m. spalio 3 d. 20 val. 38 min. 41 sek. pareiškėja telefonu kreipėsi į banką ir pranešė apie sukčiavimo atvejį. Bankas, pareiškėjai paskambinus, blokavo jos interneto banko paskyrą ir prieigą prie banko mobiliosios programėlės, o dėl pareiškėjos vardu sukurtos Paskyros2 atšaukimo nusiuntė pareiškėją į „Smart-ID" išleidėjo SK ID Solutions AS Lietuvos filialą (toliau – SK), taip pat rekomendavo dėl sukčiavimo kreiptis į teisėsaugos institucijas.

2021 m. spalio 4 d. bankas kreipėsi į lėšų gavėjo mokėjimo paslaugų teikėją „Revolut Ltd" dėl Ginčijamo mokėjimo sumos grąžinimo ir apie tai 2021 m. spalio 6 d. informavo pareiškėją žinute interneto banke.

2021 m. gruodžio 1 d. bankas gavo atsakymą iš lėšų gavėjo mokėjimo paslaugų teikėjo, kad nėra galimybės susigrąžinti Ginčijamo mokėjimo, kuris buvo įvykdytas kaip momentinis mokėjimas, lėšų, ir apie tai informavo pareiškėją žinute interneto banke.

Nesutikdama su banko sprendimu nekompensuoti nuostolių, susijusių su Ginčijamo mokėjimo įvykdymu, pareiškėja kreipėsi į Lietuvos banką. Kreipimesi teigia, kad 2021 m. spalio 3 d. gavo SMS žinutę, raginančią atnaujinti „Smart-ID" programėlę pagal pateiktą nuorodą. Paaiškindama su sukčiavimo ataka susijusias aplinkybes, lėmusias Ginčijamo mokėjimo įvykdymą, pareiškėja kreipimesi nurodo: „kadangi Smart-ID programėlėje esu aktyvavusi paslaugą apie SMS pranešimų siuntimą apie pinigų judėjimą sąskaitoje, aš atidariau gautą nuorodą, net nepagalvodama, kad ji gali būti fiktyvi. Suklastota interneto banko svetainė nieko nesiskyrė nuo tikrosios banko svetainės. Suvedžiau savo prisijungimo duomenis ir patvirtinau Smart-ID. Puslapis ilgai krovėsi, telefonas išsijungė ir aš iki galo neatlikau veiksmo." Pareiškėjos teigimu, po kelių minučių į savo mobilųjį telefoną ji gavo banko SMS žinutę, kad į jos sąskaitą banke pervesti jai nepažįstamo asmens – Y. Y., pinigai (1950 Eur). Pareiškėja nurodo tuomet supratusi, kad tapo sukčių auka – ji nedelsiant susisiekė su banku ir sužinojo, kad iš jos sąskaitos banke įvykdytas Ginčijamas mokėjimas. Pareiškėjai nesuprantama, kodėl bankas klientams leidžia naudotis identifikavimosi priemonėmis, kurias lengvai gali užvaldyti sukčiai ir pasinaudoti svetimomis sąskaitomis. Pareiškėjos manymu, bankas, neužtikrinęs jos sąskaitoje esančių lėšų saugumo, nepagrįstai atsisakė atlyginti dėl Ginčijamo mokėjimo

įvykdymo patirtus nuostolius. Pareiškėja prašė rekomenduoti bankui kompensuoti dėl sukčių naudai įvykdyto Ginčijamo mokėjimo jos patirtus nuostolius – 5 150 Eur.

Atsiliepime į pareiškėjos kreipimąsi bankas nurodo, kad nesutinka tenkinti pareiškėjos reikalavimo. Banko manymu, paspausdama neaiškią nuorodą, suvesdama savo interneto banko ID, asmens kodą ir savo mobiliajame įrenginyje atliekamus veiksmus patvirtindama tik jai žinomais Paskyros1 PIN1 ir PIN2 kodais pareiškėja elgėsi neapdairiai ir itin neatsargiai, t. y. nesilaikė atidumo ir rūpestingumo reikalavimų. Dėl to tretieji asmenys pareiškėjos vardu galėjo susikurti Paskyrą2, su kuria vėliau patvirtino Ginčijamą mokėjimą banko mobiliojoje programėlėje. Banko nuomone, pareiškėja ne tik nesilaikė 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, kuriose nustatyta „Smart-ID" naudotojo pareiga privatųjį raktą naudoti ir valdyti tik pačiam „Smart-ID" naudotojui. Tai lėmė, kad tretieji asmenys pasisavino pareiškėjos tapatybę. Pareiškėjos didelį neatsargumą, banko teigimu, rodo ir tai, kad ji nedvejodama įvedė tik jai žinomus Paskyros1 PIN1 ir PIN2 kodus trečiųjų asmenų sukurtoje interneto svetainėje, į kurią 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" išleidėją 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 Paskyros2 sukūrimo ir Ginčijamo mokėjimo įvykdymo laiko, bankas paaiškino, kad jam nėra žinoma, kaip tretieji asmenys pasirenka, kam siųsti SMS pranešimus su neaiškiomis nuorodomis. Nagrinėjamu atveju tretieji asmenys į tokią pačią sukčiavimo schemą įtraukė ir kitą banko klientą (toliau – klientas1), t. y. pirmiausia inicijavo ir patvirtino mokėjimą iš kliento1 banke esančios sąskaitos (1 950 Eur) ir šias lėšas pervedė į pareiškėjos sąskaitą. Klientui1 informavus banką apie sukčiavimą, bankas nurodo nedelsdamas išsiuntė prašymą pareiškėjai dėl lėšų grąžinimo, bet negavo jos sutikimo, kad lėšos būtų grąžintos klientui1. Dėl to tretieji asmenys sukčiaudami pasisavino ne tik pareiškėjai priklausiusias, bet ir iš kliento1 į pareiškėjos sąskaitą banke trečiųjų asmenų pervestas lėšas.

Bankas pažymi, kad operacijoms patvirtinti taiko papildomą kliento ir jo operacijų autentifikavimą, taip siekdamas klientams suteikti galimybę įsitikinti inicijuojamos operacijos teisėtumu. Klientui įvykdžius visas būtinas, banko ir kliento sutartas sąlygas, kuriomis tinkamai identifikuojama kliento inicijuota operacija, bankas įsipareigoja tokias operacijas įvykdyti. Bankas nurodė, kad vykdant Ginčijamą mokėjimą banko sistemos veikė saugiai, jokių sutrikimų nebuvo užfiksuota. Banko teigimu, Ginčijamo mokėjimo įvykdymą lėmė tai, kad pareiškėja paspaudė nuorodą į sukčių sukurtą interneto puslapį, įvedė tik jai žinomus personalizuotus duomenis, taip suteikdama galimybę sukčiams atlikti Ginčijamą mokėjimą. Banko teigimu, jis deda visas pastangas ir vykdo visus reikalavimus, kad užtikrintų klientų lėšų saugumą, tačiau neturi galimybės kontroliuoti klientų neatsargių veiksmų, kurie nėra ir negali būti banko kontroliuojami. Įvertinęs aplinkybių visumą ir teisinį reglamentavimą, bankas mano, kad neprivalo kompensuoti pareiškėjai dėl Ginčijamo mokėjimo patirtų nuostolių.

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 nustatyti ir įvertinti faktines aplinkybes dėl Lietuvos banko priežiūrimo finansų rinkos dalyvio galimo Lietuvos banko kompetencijai priskirtų teisės aktų reikalavimų pažeidimo. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Pareiškėjos ir banko ginčas kilo dėl to, kad bankas atsisakė grąžinti ir (ar) kompensuoti Ginčijamo mokėjimo, įvykdyto pareiškėjos vardu tretiesiems asmenims sukūrus Paskyrą2 jų kontroliuojamame įrenginyje, sumą. Pareiškėja mano, kad bankas nesiėmė tinkamų veiksmų, kad būtų užtikrintas jos sąskaitos ir ten esančių lėšų saugumas, todėl yra atsakingas už įvykdžius Ginčijamą mokėjimą atsiradusius nuostolius. Bankas teigia, kad tretieji asmenys įgijo

sąlygas inicijuoti ir patvirtinti Ginčijamą mokėjimą tik dėl to, kad pareiškėja dėl didelio neatsargumo atskleidė savo mokėjimo priemonių personalizuotus saugumo duomenis tretiesiems asmenims ir Paskyros 2 sukūrimą patvirtino suvesdama savo naudojamos Paskyros1 PIN kodus, todėl jis neprivalo grąžinti ir (ar) kompensuoti Ginčijamo mokėjimo lėšų sumos.

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, nustato Lietuvos Respublikos mokėjimų įstatymas. Mokėjimų įstatymo 29 straipsnio 1 dalyje nustatyta, kad mokėjimo operacija laikoma autorizuota tik tada, kai mokėtojas duoda sutikimą įvykdyti mokėjimo operaciją. Jeigu mokėtojo sutikimo įvykdyti mokėjimo operaciją nėra, laikoma, kad mokėjimo operacija yra neautorizuota (Mokėjimų įstatymo 29 straipsnio 2 dalis).

Šalys neginčija aplinkybės, kad Ginčijamą mokėjimą inicijavo ir įvykdė tretieji asmenys, neteisėtu būdu sužinoję (pasisavinę) pareiškėjos mokėjimo priemonių personalizuotus saugumo duomenis ir juos panaudoję Paskyrai2 pareiškėjos vardu sukurti, o vėliau ir pačiam Ginčijamam mokėjimui inicijuoti ir įvykdyti. Akivaizdu, kad Ginčijamo mokėjimo inicijavimas ir patvirtinimas neatitiko pareiškėjos valios, nors formaliai (pagal išorinius požymius) ir sutapo su jos ir banko sutarta sutikimo mokėjimo operacijoms davimo forma ir tvarka. Bankas neginčija pareiškėjos nurodytos aplinkybės, kad Ginčijamas mokėjimas nebuvo pareiškėjos autorizuotas, todėl Lietuvos bankas daro išvadą, kad Ginčijamas mokėjimas, atliktas nesant pareiškėjos valios, net nežinant apie mokėjimo inicijavimo aplinkybę ir neišreiškus jokių valinių veiksmų jam patvirtinti, laikytinas neautorizuotu.

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

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

Mokėjimų įstatymo 39 straipsnio 1 dalis nustato, kad mokėtojui gali tekti dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai iki 50 Eur, kai šie nuostoliai patirti dėl: 1) prarastos ar pavogtos mokėjimo priemonės panaudojimo; 2) neteisėto mokėjimo priemonės pasisavinimo. Tačiau, kaip nustatyta Mokėjimų įstatymo 39 straipsnio 2 dalyje, mokėtojas neturi patirti jokių nuostolių, jeigu 1) jis iki mokėjimo operacijos įvykdymo negalėjo pastebėti mokėjimo priemonės praradimo, vagystės arba neteisėto pasisavinimo, išskyrus atvejus, kai jis veikė nesąžiningai; 2) nuostoliai yra patirti dėl mokėjimo paslaugų teikėjo, jo darbuotojo, tarpininko, filialo ar asmenų, kuriems perduotas veiklos funkcijų valdymas, veiksmų ar neveikimo.

Mokėjimų įstatymo 39 straipsnio 3 dalyje nustatyta, kad „mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai, jeigu jis juos patyrė veikdamas nesąžiningai arba tyčia ar dėl didelio neatsargumo neįvykdęs vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų. Tokiais atvejais šio straipsnio 1 dalyje nustatytas didžiausios nuostolių sumos ribojimas netaikomas.“ Mokėjimų įstatymo 34 straipsnyje reglamentuojamos mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigos: 1) naudotis mokėjimo priemone pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas; 2) sužinojus apie mokėjimo priemonės praradimą, vagystę arba neteisėtą pasisavinimą ar neautorizuotą jos naudojimą, nedelsiant apie tai pranešti mokėjimo paslaugų teikėjui arba jo nurodytam subjektui. Mokėjimo paslaugų vartotojas, gavęs mokėjimo priemonę, privalo imtis veiksmų, kad būtų apsaugoti personalizuoti saugumo duomenys (Mokėjimų įstatymo 34 straipsnio 2 dalis).

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

sukčiavimas arba didelis neatsargumas (Mokėjimų įstatymo 37 straipsnio 3 dalis).

Įvertinus 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, kuriais patvirtinamas mokėtojo sukčiavimas (nesąžiningumas arba tyčia) arba didelis neatsargumas (Mokėjimų įstatymo 37 straipsnio 3 dalis ir 39 straipsnio 3 dalis). Duomenų, kad pareiškėja galėjo veikti nesąžiningai arba tyčia, kaip ir šalių ginčo dėl to, nėra. Tai reiškia, kad siekiant įvertinti, ar bankas pagrįstai atsisako kompensuoti pareiškėjos nuostolius, susijusius su Ginčijamo mokėjimo įvykdymu, ir ar jai galėtų būti taikoma Mokėjimų įstatymo 39 straipsnio 3 dalis, būtina nustatyti, ar pareiškėjos elgesys atskleidžiant personalizuotus jai išduotų mokėjimo priemonių požymius, taip pat kiti veiksmai, dėl kurių galėjo būti įvykdytas Ginčijamas mokėjimas, vertintini kaip didelis neatsargumas, dėl kurio reikalaujami atlyginti nuostoliai turėtų tekti jai pačiai.

Antrosios mokėjimo paslaugų direktyvos preambulės 72 punkte rašoma, kad „siekiant įvertinti galimą mokėjimo paslaugų vartotojo aplaidumą ar didelį aplaidumą, reikėtų atsižvelgti į visas aplinkybes. Įtariamo aplaidumo įrodymai ir laipsnis paprastai turėtų būti vertinami pagal nacionalinę teisę. Tačiau nors aplaidumo sąvoka reiškia, kad pažeidžiamas įsipareigojimas elgtis rūpestingai, didelis aplaidumas turėtų reikšti daugiau nei vien aplaidumą ir apimti labai nerūpestingą elgesį; pavyzdžiui, tai būtų mokėjimo operacijos autorizavimui naudojamų saugumo požymių laikymas prie mokėjimo priemonės atviru ir trečiosioms šalims lengvai atskleidžiamu formatu“. Didelio neatsargumo sąvoka plėtojama ir Lietuvos Aukščiausiojo Teismo praktikoje. Kasacinis teismas yra išaiškinęs, kad „didelis neatsargumas kaip kaltės forma pasireiškia neprotingu arba išskirtiniu rūpestingumo nebuvimu, kai asmuo nėra tiek rūpestingas, kiek akivaizdžiai būtina esamomis aplinkybėmis“.[1]

Nagrinėdamas ginčus dėl nuostolių, susijusių su neautorizuotomis mokėjimo operacijomis, įvykusiomis dėl sukčiavimo atakų, ir spręsdamas dėl mokėjimo paslaugų teikėjo atsakomybės už šių nuostolių atlyginimą nustačius, kad vartotojas (mokėtojas) teisės aktuose ir (ar) sutartyje nustatytas pareigas, susijusias su mokėjimo priemonėmis, vykdė netinkamai, Lietuvos bankas laikosi nuomonės, kad didelis neatsargumas yra vertinamojo pobūdžio aplinkybė. Tai reiškia, kad išvada, ar mokėtojo elgesį galima vertinti kaip neatsargų ar labai neatsargų, daroma kiekvienu konkrečiu atveju, įvertinus nagrinėjant ginčą nustatytų individualių, specifinių aplinkybių visumą, kurią patvirtina ginčo byloje esantys įrodymai ir (arba) šalių neginčijamos neautorizuotos mokėjimo operacijos įvykdymo aplinkybės. Taigi išvada dėl pareiškėjos, kaip mokėtojos, paprasto ar didelio neatsargumo negali būti daroma izoliuotai, t. y. išsamiai neįvertinus viso Ginčijamo mokėjimo įvykdymo ir su tuo susijusių aplinkybių konteksto.

Sprendimą nekompensuoti pareiškėjos nuostolių bankas grindžia Ginčijamo mokėjimo įvykdymą lėmusiais pareiškėjos veiksmais, kurie, banko vertinimu, rodo didelį jos neatsargumą. Banko nuomone, pareiškėja, paspausdama neaiškią nuorodą, suvesdama savo interneto banko ID, asmens kodą ir savo mobiliajame įrenginyje atliekamus veiksmus patvirtindama tik jai žinomais Paskyros1 PIN1 ir PIN2 kodais (dėl to tretieji asmenys jos vardu galėjo susikurti Paskyrą2), pažeidė jai, kaip mokėtojai, su išduotomis mokėjimo priemonėmis nustatytas pareigas, o tai reiškia, kad ji nesilaikė atidumo ir rūpestingumo reikalavimų.

Vertinamų aplinkybių kontekste būtina pažymėti, kad visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai mokėtojui tenka tik tuo atveju, jei tenkinamos abi šios 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 neautorizuoto Ginčijamo mokėjimo įvykdymo galėtų būti vertinamas kaip pagrįstas tik tuo atveju, jei būtų įrodyta, kad pareiškėja, atskleisdama personalizuotus savo mokėjimo priemonių saugumo duomenis ir taip suteikdama galimybę tretiesiems asmenims panaudoti šiuos duomenis Paskyrai2 sukurti, o vėliau ir inicijuoti bei patvirtinti Ginčijamą mokėjimą, elgėsi itin aplaidžiai, t. y. buvo labai neatsargi.

Lietuvos bankas, siekdamas nustatyti, ar pareiškėjos elgesys gali būti laikomas dideliu neatsargumu, vertino ne tik tai, kad pati pareiškėja, pasitikėdama į mobilųjį telefoną gautame SMS pranešime nurodyta informacija, paspaudė pateiktą nuorodą, suvedė savo prisijungimo prie interneto banko ir kitus duomenis suklastotame banko interneto banko puslapyje ir savo naudojamos tapatybės priemonės Paskyros1 PIN1 ir PIN2 slaptažodžius, bet ir kokių veiksmų

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

prevenciškai ėmėsi ir imasi bankas, kad mokėjimo paslaugos elektroninėje erdvėje būtų teikiamos saugiai, o vartotojai būtų tinkamai supažindinti su sukčiavimo elektroninėje erdvėje rizikomis, tapatybės patvirtinimo priemonės saugaus naudojimo, personalizuotų saugumo žymenų suvedimo ir atskleidimo reikšme ir teisinėmis pasekmėmis. Vertinant pareiškėjos elgesį, svarbu nustatyti, kaip ji buvo įtikinta atskleisti savo mokėjimo priemonės personalizuotus saugos ir kitus duomenis, kad būtų sukurta Paskyra2, suteikusi galimybę tretiesiems asmenims be pareiškėjos žinios ir valinių veiksmų inicijuoti bei patvirtinti Ginčijamą mokėjimą.

Nagrinėjant ginčą nustatyta, kad pareiškėja į savo mobilųjį telefoną gavo trečiųjų asmenų siųstą tokio turinio SMS pranešimą: „Jusu SEB paskyra buvo itraukta i karantino zona, reikia is naujo patvirtinti. Uzkirsti kelia karantinui, jus turite atlikti siuos veiksmus cia: HK38721.com“. Supratusi, kad yra įspėjama dėl „Smart-ID“ paskyros įtraukimo į karantino zoną ir informuojama apie būtinybę atnaujinti šią paskyrą paspaudžiant SMS pranešime pateiktą nuorodą, pareiškėja paspaudė šią nuorodą ir atsidariusiame trečiųjų asmenų sukurtame suklastotame banko interneto banko tinklalapyje suvedė savo interneto banko atpažinimo kodą (ID), asmens kodą ir, savo mobiliajame įrenginyje į savo naudojamą Paskyrą1 gavusi patvirtinimo kodus, suvedė šios paskyros PIN1 ir PIN2 kodus. Šiais kodais 20.22 val. patvirtintas sutikimas pareiškėjos vardu sukurti Paskyrą2 trečiųjų asmenų valdomame įrenginyje.

Vystantis ir tobulėjant technologijoms, vystomi 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 aukštas 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 sukčiavimo ataka, per kurią įvykdyta tapatybės vagystė, t. y. pasisavinti pareiškėjos mokėjimo priemonių personalizuoti saugumo ir pačios pareiškėjos asmens duomenys, kad tretieji asmenys įgytų galimybę sukurti jos vardu naują tapatybės patvirtinimo priemonės „Smart-ID“ paskyrą ir per ją užvaldytų pareiškėjos sąskaitą banke, inicijuotų ir patvirtintų Ginčijamą mokėjimą, buvo ganėtinai sofistikuota. Taikant socialinės inžinerijos metodus, sukurtas tiek poreikis veikti neatidėliotinai, kad būtų galima naudotis banko teikiamomis paslaugomis, tiek ir įtikinamai pasitelkta aplinka (suklastota banko interneto banko svetainė), sukūrusi pirminį tikrumo įspūdį ir skatinusi pasitikėjimą bei mažinusi racionalias, pagrįstas abejones dėl nurodymų atskleisti ir suvesti savo mokėjimo priemonių ir asmens duomenis pagrįstumo. Dėl to manytina, kad mokėjimo paslaugų teikėjai, kaip savo srities profesionalai, turi dėti reikiamas pastangas, kad nuolat kryptingai ir tinkamai informuotų savo klientus (vartotojus) apie sukčiavimo pavojus ir rizikas, susijusias su sukčiavimais elektroninėje erdvėje, ir primintų, kokie ir kaip vartotojų duomenys turėtų būti saugomi ir neatskleisti tretiesiems asmenims.

Vertinant banko veiksmus, kurių jis ėmėsi, kad informuotų savo klientus, tarp jų ir pareiškėją, apie elektroninėje erdvėje kylančias rizikas naudojantis mokėjimo paslaugomis, pažymėtina, kad Bendrųjų taisyklių sąlygose, kurios yra neatskiriama ginčo šalių sutartinių santykių dalis, ar kituose šalių sutartinius santykius reguliuojančiuose dokumentuose nepaaiškinta tapatybės patvirtinimo priemonės „Smart-ID“, PIN kodų suvedimo reikšmė vykdant mokėjimo operacijas ir šių kodų panaudojimo galimos pasekmės klientui. Taigi ginčo byloje nėra duomenų, kad pareiškėja buvo tinkamai supažindinta su informacija, kokius veiksmus, naudodamasi „Smart-ID“ programėle, ji gali atlikti, taip pat kokie veiksmai ir 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“ nurodyta, kad „Smart-ID“ „gali būti naudojama norint saugiai prisijungti prie interneto banko, tvirtinti mokėjimus, naudotis trečiųjų šalių paslaugų teikėjų paslaugomis ir pasirašyti elektroninius dokumentus. Prilygsta elektroniniam parašui“.

Bankas, paaiškindamas klientų supažindinimą su programėlės „Smart-ID“ naudojimosi ypatumais, nurodė, kad klientai, elektroninio parašo „Smart-ID“ naudotojai, tvirtindami savo tapatybę (naudojamas PIN1 kodas) ar jungdamiesi prie informacinių išteklių, mato veiksmo, t. y. tapatybės tvirtinimo, užklausos pavadinimą „Prisijungimas“ arba „Login“ ir „Patvirtinimas“

(naudojamas PIN2 kodas). Pasirašyti elektroninius dokumentus (paraiškas, sutartis ir kt.), kaip nurodo bankas, naudojamas būtent elektroninio parašo „Smart-ID" PIN2 kodas. Bankas taip pat atkreipia dėmesį, kad SK savo interneto svetainėje „Smart-ID" vartotojams pateikia informaciją, kurioje aiškiai nurodyta „Smart-ID" PIN kodų ir veiksmų su programėle „Smart-ID" reikšmė, t. y. kad PIN1 naudojamas tapatybės patvirtinimui, o PIN2 skirtas elektroniniam parašui[2].

Vis dėlto būtina atkreipti dėmesį, kad, banko pateiktais duomenimis[3], „Smart-ID" pranešimuose, kuriais pareiškėjos buvo prašoma suvesti PIN1 ir PIN2 kodus, be kontrolinio kodo, buvo rodomi tik prašomus atlikti veiksmus identifikuojantys bendro pobūdžio reikšmę turintys žodžiai „Prisijungimas" (suvedant PIN1 kodą) ir „Patvirtinimas" (suvedant PIN2 kodą), jokiais kitais papildomais požymiais neaprašant, nedetalizuojant veiksmo, kuriam tvirtinti prašoma suvesti PIN2 kodą. Atsižvelgiant į tai, kad šalių sutartinius santykius reglamentuojančiuose dokumentuose nenurodyta, kokius veiksmus pareiškėja, naudodamasi „Smart-ID" programėle, gali atlikti, negalima teigti, kad pareiškėja matė ir suprato ar turėjo suprasti, kokiam veiksmui išreiškia sutikimą, suvesdama Paskyros1 PIN2 kodą. Pažymėtina, kad Paskyra2 pareiškėjos vardu buvo sukurta elektroninio banko sąsajos tapatybės patvirtinimo įrankiu, t. y. Paskyra1, pačiai pareiškėjai nežinant ir neturint duomenų, kad pareiškėja būtų tinkamai informuota, jog per banko interneto banką ji gali susikurti naują tapatybės patvirtinimo priemonę – „Smart-ID Basic"[4] paskyrą naujame galiniame įrenginyje, kad galėtų naudotis banko teikiamomis elektroninės bankininkystės paslaugomis.

Kita vertus, nors ginčo byloje nėra duomenų, kad bankas asmeniškai supažindino pareiškėją su naudojamos tapatybės patvirtinimo priemonės „Smart-ID" ir jos PIN kodų suvedimo teisine reikšmetarp šalių susiklosčiusiuose sutartiniuose santykiuose ar o pareiškėją susukčiavimo elektroninėje erdvėje naudojantis mokėjimo paslaugomis rizika, neabejotina, 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. Lėšų ir atliekamų mokėjimo operacijų, kaip ir kitų elektroninėje erdvėje teikiamų mokėjimo paslaugų, saugumas priklauso ir nuo tinkamo mokėjimo paslaugų vartotojų pareigų, susijusių su mokėjimo priemonių naudojimu, vykdymo. Kaip minėta, Mokėjimų įstatymo 34 straipsnyje nustatyta viena iš mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigų – naudotis mokėjimo priemone pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas. Banko Bendrųjų taisyklių 1 priedo 10 skyriuje nurodyta, kad banko suteiktą mokėjimo priemonę ir su ja susijusius personalizuotus saugumo duomenis mokėtojas privalo saugoti ir imtis visų reikiamų veiksmų, kad personalizuoti saugumo duomenys nebūtų atskleisti jokiems kitiems asmenims. Be to, pagal banko Paslaugų interneto banke teikimo sąlygų aprašą, 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, klientas privalo apie tai nedelsdamas pranešti teisėsaugos institucijoms. Už atpažinimo priemonių saugojimą ir tinkamą naudojimą, neatskleidimą tretiesiems asmenims yra atsakingas klientas. Paslaugų interneto banke teikimo sąlygų aprašas, be kita ko, nustato, kad klientas įsipareigoja laikyti paslaptyje atpažinimo kodą, slaptažodžius, PIN kodus, neužrašyti jų ant generatoriaus ar kitų kartu su juo laikomų daiktų ir jokia kita forma neatskleisti ar nepadaryti jų prieinamų tretiesiems asmenims (20.4 ir 38 punktai).

Aptartos banko Bendrųjų taisyklių ir Paslaugų interneto banke teikimo sąlygų aprašo nuostatos, nors ir nedetalizuoja tapatybės patvirtinimo priemonės „Smart-ID" ir jos PIN kodų suvedimo teisinės reikšmės inicijuojant ir patvirtinant mokėjimo nurodymus įvykdyti mokėjimo operacijas, tačiau aiškiai nustato, kad už tapatybės patvirtinimo priemonės personalizuotų saugumo duomenų konfidencialumą atsako mokėtojas. Atsižvelgiant į tai, manytina, kad pareiškėjos elgesys galėtų būti laikomas atitinkančiu mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas tik nustačius, jog ji ėmėsi adekvačių veiksmų (ar priešingai, nustačius, kad nuo tam tikrų veiksmų susilaikė), siekdama tinkamai užtikrinti banko

---

[2] https://www.smart-id.com/lt/pagalba/duk/registracija/kam-yra-reikalingi-du-pin-kodai.

[3] Kartu su papildomais paaiškinimais bankas pateikė duomenis, kokio turinio „Smart-ID" pranešimai, prašant suvesti PIN1 ir PIN2 kodus, buvo siunčiami banko klientams, taip pat ir pareiškėjai, tuo metu, kai buvo sukurta „Smart-ID" Paskyra2.

[4] „Smart-ID Basic" paskyros ribojamos tik elektronine bankininkyste https://www.smart-id.com/lt/pagalba/duk/registracija/smart-id-registracijos-budai/.

išduotų mokėjimo priemonių personalizuotų saugumo duomenų, sudarančių sąlygas inicijuoti ir tvirtinti mokėjimus, konfidencialumą.

Įvertinus ginčo byloje esančius duomenis ir nustatytas aplinkybes, negalima daryti išvados, kad pareiškėjos elgesys atitiko banko nustatytas naudojimosi mokėjimo priemonėmis sąlygas ar buvo adekvatus ir pakankamas su mokėjimo priemonių personalizuotų saugumo duomenų konfidencialumo užtikrinimu susijusioms pareigoms tinkamai įvykdyti. Nors į mobilųjį telefoną atsiųsta SMS žinutė galėjo sudaryti įspūdį, kad yra iš banko, nes buvo siųsta banko vardu, tačiau tai, kad pareiškėja iki personalizuotų duomenų atskleidimo (pateikimo suklastotoje interneto svetainėje) nesudvejojo pranešime nurodytos informacijos ir paspaudus nuorodą atsidariusios interneto svetainės patikimumu, taip pat nekvestionuodama pateiktų nurodymų pagrįstumo suvedė savo naudojamos Paskyros1 PIN1 ir PIN2 slaptažodžius, kai atsirado tai padaryti raginantys „Smart-ID" programėlės pranešimai, leidžia teigti, kad jos elgesys nebuvo itin apdairus ir atsargus.

Sprendžiant dėl pareiškėjos neatsargumo laipsnio, atkreiptinas dėmesys į tai, kad trečiųjų asmenų atsiųsta SMS žinutė, parašyta ne lietuviškais rašmenimis, informavo pareiškėją apie tai, kad jos „SEB paskyra buvo įtraukta į karantino zoną" ir tam, kad pareiškėja užkirstų kelią tariamam banko paskyros karantinui, ji, vadovaudamasi SMS žinutės nurodymais, turi spausti pateiktą nuorodą. Vertinant žinutės turinį, nėra aišku, kas konkrečiai turima omenyje ir kaip galima būtų interpretuoti, vertinti teiginio „SEB paskyra buvo įtraukta į karantino zoną" prasmę, nes tokių procesų nereglamentuoja nei teisės aktai, nei banko parengtos taisyklės ar kiti dokumentai. Pateikdama paaiškinimus dėl SMS žinutės turinio, pareiškėja nurodė, kad iš banko anksčiau yra gavusi elektroninio pašto pranešimų, informuojančių apie būtinybę atnaujinti savo banko paskyrą. Dėl to ir šį kartą pamaniusi, kad taip bankas ją ragina atnaujinti savo interneto banko paskyrą. Pareiškėja taip pat maniusi, kad dėl šalyje įvesto karantino bankas griežtina naudojimosi elektroninės bankininkystės paslaugomis sąlygas, todėl ji, norėdama ir toliau naudotis banko išduota mokėjimo kortele ir interneto banku, turi skubiai atnaujinti savo interneto banko paskyrą. Vis dėlto, atsižvelgus į žinutės turinį, manytina, kad subjektyvūs pareiškėjos pasvarstymai apie SMS žinutės teksto reikšmę nevisiškai atitinka pateiktą informaciją ir nurodymus. Atkreiptinas dėmesys, kad SMS žinutė informavo pareiškėją apie jos banko paskyros įtraukimą į „karantino zoną" ir ragino spausti nuorodą, kad būtų užkirstas kelias tariamam jos banko paskyros įtraukimui į „karantino zoną". Taigi žinutėje nebuvo teiginių apie tai, kad bankas taiko apribojimus teikiamoms mokėjimo paslaugoms dėl šalyje įvesto karantino ir, neatnaujinusi banko interneto banko paskyros, pareiškėja negalės naudotis banko teikiamomis paslaugomis. Tačiau nei ši aplinkybė, nei tai, kad žinutė parašyta ne lietuviškais rašmenimis ir pateko ne į bendrą kitų banko siųstų žinučių srautą, nesukėlė pareiškėjai jokių abejonių. Priešingai, pareiškėja teigė nesuabejojusi siuntėjo autentiškumu, nedvejodama paspaudusi pateiktą nuorodą ir suvedusi savo mokėjimo priemonių personalizuotus saugumo duomenis, o vėliau ir savo naudojamos Paskyros1 PIN kodus.

Paaiškindama personalizuotų saugumo duomenų suvedimo suklastotoje banko interneto svetainėje aplinkybes, pareiškėja nurodė, kad paspaudus žinutėje pateiktą nuorodą atsidariusi interneto svetainė niekuo nesiskyrė nuo tikros banko interneto banko svetainės. Pareiškėjos teigimu, joje buvo prašoma suvesti prisijungimo prie interneto banko duomenis ir slaptažodį, peržiūrėti ir patvirtinti vardą ir pavardę, gyvenamosios vietos adresą. Pareiškėja nurodė, kad, paspaudus mygtuką „Patvirtinti", „labai ilgai sukosi, internetas vis galvojo", tad negavusi jokio patvirtinimo ji išjungė tą interneto langą. Taigi aplinkybė, kad, suvedus visus prašomus personalizuotus saugumo duomenis ir patvirtinus atliekamus veiksmus (t. y. nurodytą informaciją) Paskyros1 PIN kodais, prieiga prie interneto banko paskyros vis tiek tinkamai neveikė, pareiškėjai, kuri žinutėje pateiktą nuorodą paspaudė siekdama atnaujinti savo interneto banko paskyrą dėl banko tariamai taikomų apribojimų paslaugų teikimui karantino metu, nesukėlė abejonių ir ji tiesiog uždarė interneto naršyklės langą. Pažymėtina ir tai, kad pareiškėjos naudotos Paskyros1 PIN kodais buvo patvirtintas Paskyros2 sukūrimas trečiųjų asmenų naudojamame galiniame įrenginyje, o apie tai pareiškėja buvo iškart[5] informuota banko

[5] Ginčo byloje esančiais duomenimis, Paskyra2 pareiškėjos vardu trečiųjų asmenų naudojamame galiniame įrenginyje buvo sukurta 20.22 val., o bankas apie pareiškėjos vardu kuriamą Paskyrą2 informavo pareiškėją 20.23 val. 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. (*duomenys neskelbtini*). SEB bankas". Apie kuriamą Paskyrą2 bankas pareiškėją tuo pačiu metu (t. y. 20.23 val.) papildomai informavo pareiškėjos el. pašto adresu (*duomenys neskelbtini*). Banko duomenimis, tą patvirtina ir pareiškėjos kartu su kreipimusi pateiktos ekrano nuotraukos, pareiškėją apie kuriamą Paskyrą2 el. paštu informavo ir „Smart-ID" programėlės išleidėjas SK.

SMS žinute, taip pat banko ir SK elektroninio pašto pranešimais, tačiau jų nepatikrino ir (ar) neperskaitė iki kito banko siųsto pranešimo apie į pareiškėjos banko sąskaitą pervestas kliento1 lėšas.

Aptariamų aplinkybių kontekste svarbu įvertinti ir trečiųjų asmenų siųstoje SMS žinutėje pateiktą nuorodą – *HK38721.com*. Nagrinėdamas dėl neautorizuotų mokėjimo operacijų, atliktų įvykus sukčiavimo atakai, kilusius ginčus Lietuvos bankas yra pažymėjęs, kad vien faktas, jog vartotojas paspaudė jam SMS žinute atsiųstą aktyvią nuorodą ir nepastebėjo, kad pateko ne į tikrą banko interneto puslapį, o į trečiųjų asmenų suklastotą banko interneto puslapį, savaime nereiškia vartotojo didelio neatsargumo. Vis dėlto būtina atkreipti dėmesį į tai, kad SMS žinutėje pateikta aktyvi nuoroda buvo visiškai nepanaši į tikrąją banko interneto banko nuorodą. Jos pavadinime nebuvo jokio panašumo į jungiantis prie banko interneto banko matomą informaciją (pvz., nurodytas klaidingas banko pavadinimas, kuris vizualiai galėtų atrodyti panašus į tikrąjį banko pavadinimą ir pan.). Manytina, kad ši aplinkybė, kuri vidutiniškai apdairų ir rūpestingą vartotoją būtų privertusi rimtai sudvejoti atliekamų veiksmų ir pateiktų prašymų pagrįstumu, pareiškėjai galėjo nesukelti jokių abejonių tik dėl to, kad ji buvo itin neatidi.

Kaip minėta, kiekvienu konkrečiu atveju išvada dėl mokėtojo elgesio pripažinimo neatsargiu ar labai neatsargiu daroma įvertinus nustatytų individualių, specifinių aplinkybių visumą, kurią patvirtina ginčo byloje esantys įrodymai ir (arba) šalių neginčijamos neautorizuotos mokėjimo operacijos įvykdymo aplinkybės. Vis dėlto, šiuo atveju ginčo nagrinėjimo metu nustatytos ir pirmiau analizuotos aplinkybės, susijusios tiek su pačios sukčiavimo atakos pobūdžiu, tiek su banko veiksmais, o svarbiausia – susijusios su pačios pareiškėjos veiksmais, ir būtent šių aplinkybių visuma, net įvertinus ir tai, kad nagrinėjamo ginčo kontekste aktuali sukčiavimo ataka buvo ganėtinai sofistikuota ir ją pastebėti buvo būtinas pareiškėjos atidumas ir rūpestingumas, nesudaro pagrindo vertinti pareiškėjos elgesio tik kaip neatsargaus. Pareiškėja kritiškai neįvertino gautos SMS žinutės turinio, paspaudė joje pateiktą nuorodą ir suklastotoje banko interneto banko svetainėje suvedė personalizuotus saugumo duomenis ir nedvejojusi suvedė savo Paskyros1 PIN kodus tik dėl to, kad nebuvo atsargi ir rūpestinga, kiek akivaizdžiai buvo būtina vertinamomis aplinkybėmis. Taigi pareiškėja ne tik netinkamai vykdė Mokėjimų įstatyme nustatytas pareigas, susijusias su jai išduotomis mokėjimo priemonėmis ir jų personalizuotais saugumo duomenimis, bet ir tai darė elgdamasi labai neatsargiai. Tai reiškia, kad pareiškėjos elgesys nebuvo toks, koks akivaizdžiai buvo būtinas, o tai lėmė, kad tretieji asmenys įgijo galimybę pareiškėjos vardu sukurti naują Paskyrą2 ir ja naudodamiesi inicijuoti bei patvirtinti Ginčijamą mokėjimą, pačiai pareiškėjai savo valios tokiai mokėjimo operacijai neišreiškus ir nežinant net apie jos inicijavimo aplinkybę.

Konstatavus, kad pareiškėja, nesilaikydama Mokėjimų įstatyme ir sutartyje su banku nustatytų pareigų, susijusių su jai išduotomis mokėjimo priemonėmis, elgėsi labai neatsargiai, darytina išvada, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, pagal kurią tokiu atveju mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai. Dėl to, Lietuvos banko vertinimu, bankas neprivalo grąžinti (kompensuoti) pareiškėjai neautorizuoto Ginčijamo mokėjimo lėšų.

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

Pareiškėja kreipimesi, be kita ko, teigia, kad „Kol bandžiau prisiskambinti, iš mano sąskaitos buvo pavogta 5 150 Eur.

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

Vis dėlto, ginčo byloje nustatytais duomenimis[6], Ginčijamas mokėjimas buvo įvykdytas 2021 m. spalio 3 d.20 val. 37 min. 37 sek., o pareiškėja į banką paskambino 20 val. 38 min. 41 sek. (banko darbuotoja atsiliepė 20 val. 39 min. 5 sek.). Taigi Ginčijamas mokėjimas iš pareiškėjos sąskaitos buvo įvykdytas dar iki pareiškėjos skambučio į banką ir pranešimo apie mokėjimo priemonės paradimą ir neautorizuotą jos panaudojimą.

[6] Banko kartu su atsiliepimu pateikti banko informacinių sistemų žurnalo duomenys.

Pareiškėjos teigimu, keistai atrodo aplinkybė, jog sukčiavimo ataka įvykdyta būtent tada, kai į jos asmeninę sąskaitą buvo pervesta 1 500 Eur. Vis dėlto šiuo atveju sutiktina su banko atsiliepimo argumentu, kad tokia pareiškėjos nurodyta aplinkybė niekaip nepaaiškina trečiųjų asmenų motyvų dėl įvykdytos sukčiavimo atakos būdo ir laiko konkretaus pasirinkimo ir pati savaime niekaip nepagrindžia pareiškėjos teiginio, kad bankas galėjo netinkamai veikti, užtikrindamas pareiškėjos banko sąskaitoje esančių lėšų saugumą.

Dėl banko teikiamų mokėjimo paslaugų saugumo

Grįsdama reikalavimą kompensuoti su Ginčijamo mokėjimo įvykdymu susijusius nuostolius pareiškėja nurodė, kad bankas, jos vertinimu, nesiėmė reikiamų veiksmų, kad užtikrintų jos sąskaitoje esančių lėšų saugumą.

Kaip minėta, Lietuvos bankas, nagrinėdamas ginčą, neatlieka patikrinimų, skirtų nustatyti, ar nebuvo pažeisti finansų įstaigų veiklai keliami teisės aktų reikalavimai. Lietuvos bankas sprendimą priima remdamasis ginčo šalių pateiktais konkrečiais įrodymais. Atsižvelgiant į tai, būtina konstatuoti, kad ginčo byloje nėra duomenų, galinčių patvirtinti pareiškėjos nurodytą aplinkybę, kad bankas nesiėmė reikiamų veiksmų, kad būtų apsaugotas jos sąskaitos ir joje esančių lėšų saugumas, o įvykdydamas Ginčijamą mokėjimą būtų pažeidęs finansų rinką reglamentuojančių teisės aktų reikalavimus.

Pateikdamas paaiškinimus dėl pareiškėjos teiginių, susijusių su banko sistemų saugumu, bankas pažymėjo, kad vykdant Ginčijamą mokėjimą nebuvo užfiksuota banko sistemų sutrikimų ar sulėtėjimo, bankas negavo pranešimų ir iš SK apie „Smart-ID" programėlės veikimo sutrikimus. Vien aplinkybė, kad Ginčijamas mokėjimas įvykdytas, pareiškėjos teigimu, sukčių naudai, savaime nepagrindžia to, kad banko taikytos saugumo priemonės (net jei ir būtų nustatyta, kad pareiškėja su jai išduotomis mokėjimo priemonėmis ir personalizuotais saugumo duomenimis elgėsi itin apdairiai) buvo ne tik nepakankamos, bet ir neatitinkančios teisės aktų reikalavimų ir tai galėjo nulemti tiek Paskyros2 sukūrimą, tiek ir paties Ginčijamo mokėjimo įvykdymą (dėl to galėtų kilti banko civilinė atsakomybė). Kaip minėta, duomenų, kad bankas nevykdė finansų rinką reglamentuojančių teisės aktų reikalavimų, nagrinėjant ginčą nenustatyta. Priešingai, įvertinus nustatytas aplinkybes, padaryta išvada, kad pareiškėjos nuostolius dėl Ginčijamo mokėjimo įvykdymo, tretiesiems asmenims sukūrus Paskyrą2, nulėmė būtent pačios pareiškėjos itin neatsargūs veiksmai.

Atsižvelgiant į nustatytas aplinkybes ir į tai, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, darytina išvada, kad pareiškėjos reikalavimas bankui grąžinti Ginčijamo mokėjimo lėšas yra nepagrįstas, todėl atmetamas.

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

Atmesti pareiškėjos X. X. reikalavimą.

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