



**LIETUVOS BANKO
TEISĖS IR LICENCIJAVIMO DEPARTAMENTO
DIREKTORIUS**

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

2025-12-17 Nr. 429-308
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:

2025 m. kovo 7 d. iš pareiškėjos banko sąskaitos buvo atlikta 997 Eur mokėjimo operacija (toliau – ginčijama mokėjimo operacija) lėšų gavėjui *Tompay LTD* (toliau – lėšų gavėjas).

Ginčo byloje nustatyta, kad pareiškėja per platformą *skelbiu.lt* gavo nepažįstamo pirkėju prisistačiusio asmens žinutę, kad jis siekia įsigyti parduodamą prekę pagal pareiškėjos įkeltą skelbimą. Pareiškėjai tariamas pirkėjas per „Viber“ pokalbių programėlę pateikė aktyvią nuorodą į suklastotą *Omniva* interneto puslapį, tikslu, kad pareiškėja patvirtintų lėšų į jos banko sąskaitą įskaitymą.

Paspaudusi aktyvią nuorodą, pareiškėja, tikslu gauti lėšas į savo banko sąskaitą, suvedė savo banko atpažinimo kodą, asmens kodą bei Smart-ID PIN1 kodą, kuriuo patvirtino trečiųjų asmenų prisijungimą prie pareiškėjos interneto banko. Pareiškėjai suvedus minėtus duomenis, tretieji asmenys prisijungė prie pareiškėjos interneto banko paskyros ir inicijavo ginčijamą mokėjimo operaciją, kurią pareiškėja patvirtino, suveddama Smart-ID PIN2 kodą.

Remdamasis visa surinkta informacija, bankas priėmė sprendimą atsisakyti pareiškėjai atlyginti jos patirtus nuostolius, nes nustatė, kad ginčijama mokėjimo operacija buvo įvykdyta panaudojus tik pareiškėjai žinomus personalizuotus saugos duomenis bei pačiai pareiškėjai suvedus savo Smart-ID PIN1 ir PIN2 kodus. Banko vertinimu, pareiškėja dėl savo didelio neatsargumo atskleidė savo mokėjimo priemonės duomenis tretiesiems asmenims, todėl patyrė nuostolių. Pareiškėja su tuo nesutiko, todėl tarp šalių kilo ginčas.

Kreipimesi į Lietuvos banką pareiškėja prašo įpareigoti banką grąžinti ginčijamos mokėjimo operacijos metu iš pareiškėjos banko sąskaitos nurašytas lėšas, t. y. grąžinti 997 Eur. Pareiškėja Lietuvos bankui paaiškino, kad „2025 m. kovo 7 d. 17:42 val. tapau finansinio sukčiavimo auka – per *skelbiu.lt* pardavinėjau prekę ir gavau žinutę iš asmens, apsimetusio pirkėju, su nuoroda į suklastotą „Omniva“ puslapį, neva prekę pirkėjas paims per kurjerių tarnybą. Buvau įtikinta, kad ten reikia suvesti savo duomenis, kad gaučiau pinigų už prekę. Apgaulės būdu suvedžiau prisijungimo prie el. bankininkystės duomenis į vizualiai identišką svetainę ir patvirtinau mokėjimą, kuris, kaip paaiškėjo, buvo neteisėtas pavedimas 997 EUR sumai į sukčiaus sąskaitą. Tai yra sukčiavimo būdu išgautas mano sutikimas suvesti savo duomenis, todėl teisiškai tai yra neautorizuotas mokėjimas. Buvai sukčių suklaidinta ir visus veiksmus dariau tikėdamasi, kad tai susiję su prekės pardavimu ir jos išsiuntimu. Tai nėra tyčinis mano veiksmas ar sąmoningas duomenų atskleidimas“.

Pareiškėja nurodo, kad į banką dėl ginčijamos mokėjimo operacijos atšaukimo kreipėsi, kai dar lėšos iš jos banko sąskaitos nebuvo nurašytos, todėl, pareiškėjos nuomone, bankas galėjo atšaukti ginčijamos mokėjimo operacijos vykdymą.

Pareiškėja taip pat teigė, kad bankas jai nesuteikė jokios informacijos apie pradėtą tyrimą, iki kovo 28 d. su pareiškėja nesusiekė, nesuteikė aiškių duomenų, kokie tikslūs veiksmai buvo atlikti dėl pavedimo stabdymo ar lėšų susigrąžinimo bei atsisakė atlyginti pareiškėjos patirtus nuostolius.

Atsiliepime į pareiškėjos kreipimąsi bankas nurodo nesutinkąs su pareiškėjos reikalavimu ir prašo jį atmesti. Bankas paaiškino, kad pareiškėja dėl didelio neatsargumo neišsaugojo savo

personalizuotų saugos duomenų, todėl tretieji asmenys jais galėjo pasinaudoti ir be pareiškėjos žinios inicijuoti ginčijamą mokėjimo operaciją. Banko teigimu, pareiškėjos didelis neatsargumas pasireiškė tuo, kad pareiškėja, prieš vesdama savo Smart-ID PIN1 ir PIN2 kodus, nesigilino į banko jai rodytą informaciją apie tikslą, kodėl jos buvo prašoma suvesti minėtus duomenis. Bankas paaiškino, kad, banko sistemų duomenimis, prieš vedant Smart-ID PIN1 kodą, pareiškėjai buvo pateikta tokia žinutė: „*Jungiatės prie SEB interneto banko*“. Pareiškėja suvedė Smart-ID PIN1 kodą ir taip davė sutikimą tretiesiems asmenims prisijungti prie pareiškėjos interneto banko paskyros.

Tretieji asmenys prisijungę prie pareiškėjos interneto banko paskyros, inicijavo dvi mokėjimo operacijas, kurias pareiškėja patvirtino du kartus suveddama savo Smart-ID PIN2 kodą. Tačiau vieną iš trečiųjų asmenų inicijuotų mokėjimo operacijų, banko saugumo sistemos sustabdė, todėl pareiškėja išvengė didesnių nuostolių.

Banko sistemų turimais duomenimis, bankas prieš pareiškėjai suvedant Smart-ID PIN2 kodą, rodė tiek ginčijamos mokėjimo operacijos sumą, tiek ir gavėjo duomenis „997,00 EUR i saskaita ****2701“, tačiau pareiškėja ir šio banko siūsto pranešimo nepaisė ir toliau tęsė trečiųjų asmenų nurodymus, taip patvirtindama ginčijamos mokėjimo operacijos įvykdymą.

Bankas paaiškino, kad pareiškėja į banką kreipėsi iš karto po to, kai patvirtino ginčijamos mokėjimo operacijos įvykdymą, tačiau bankas ginčijamos mokėjimo operacijos atšaukti jau negalėjo, nes buvo pasibaigęs mokėjimo operacijos atšaukimo momentas.

Bankas teigia ir tai, kad, rūpindamasis lėšų saugumu, periodiškai informuoja savo klientus, įskaitant ir pareiškėją, apie dažniausiai pasitaikančias sukčiavimo atakas bei primena, kokios yra saugaus naudojimosi banko teikiamomis el. paslaugomis rekomendacijos.

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 44 punktu, vartojimo ginčai Lietuvos banke nagrinėjami laikantis rungimosi, ginčų nagrinėjimo operatyvumo, koncentracijos, ekonomiškumo ir bendradarbiavimo principų. Vartotojas ir finansų rinkos dalyvis privalo įrodyti tas aplinkybes, kuriomis remiasi kaip savo reikalavimų arba atsikirtimų pagrindu, išskyrus atvejus, kai remiamasi aplinkybėmis, kurių nereikia įrodinėti. Nagrinėdamas vartojimo ginčą, Lietuvos bankas neatlieka Lietuvos Respublikos Lietuvos banko įstatymo 42¹ straipsnyje reglamentuotų patikrinimų faktinėms aplinkybėms dėl Lietuvos banko kompetencijai priskirtų teisės aktų reikalavimų laikymosi ir (arba) vartotojo įtariamo galimo šių reikalavimų pažeidimo nustatyti ir įvertinti. Nagrinėdamas ginčą, Lietuvos bankas atlieka ginčo šalių pateiktų įrodymų vertinimą ir jo pagrindu priima sprendimą.

Pareiškėjos ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjai ginčijamos mokėjimo operacijos metu iš jos sąskaitos banke pervestą sumą. Pareiškėja neigia autorizavusi ginčijamą mokėjimo operaciją ir teigia, kad bankas galėjo atšaukti ginčijamos mokėjimo operacijos įvykdymą. Banko teigimu, pareiškėjos veiksams būdingas didelis neatsargumas, todėl bankas negali būti įpareigotas pareiškėjai grąžinti ginčijamos mokėjimo operacijos 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, reglamentuoja Lietuvos Respublikos mokėjimų įstatymas.

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

Aplinkybės, kad ginčijama mokėjimo operacija nėra pareiškėjos autorizuota, o pareiškėjos personalizuotus saugumo duomenis tretieji asmenys gavo apgaulės būdu, bankas atsiliepime neginčia. Priešingai, bankas savo paaiškinimuose nurodo, kad dėl pareiškėjos atskleistų duomenų tretieji asmenys įgijo galimybę inicijuoti ginčijamą mokėjimo operaciją. Dėl šios priežasties yra akivaizdu, kad ginčijamos mokėjimo operacijos inicijavimas ir patvirtinimas neatitiko pačios pareiškėjos valios, nors formaliai (pagal išorinius požymius) ir sutapo su pareiškėjos ir banko sutarta sutikimo atlikti mokėjimo operacijas davimo forma ir tvarka. Atsižvelgdamas į tai, Lietuvos bankas daro išvadą, kad ginčijama mokėjimo operacija, atlikta nesanant pareiškėjos valios, laikytina neautorizuota.

Siekdamas išspręsti tarp šalių kilusį ginčą ir įvertinti pareiškėjos bankui keliamo reikalavimo pagrįstumą, Lietuvos bankas vertins, ar bankas: 1) atsisakydamas grąžinti pareiškėjai ginčijamos mokėjimo operacijos metu pervestas lėšas, pagrįstai rėmėsi Mokėjimų įstatymo 39 straipsnio 3 dalimi; 2) turėjo pareigą atšaukti mokėjimo operaciją.

1. Dėl neautorizuotos mokėjimo operacijos pasemių ir pareiškėjos teisės į ginčijamą mokėjimo operacijos sumos grąžinimą

Mokėjimų įstatymo 39 straipsnio 3 dalyje nustatyta, kad mokėtojai tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai, jeigu jis juos patyrė veikdamas nesažiningai arba tyčia ar dėl didelio neatsargumo neįvykdęs vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų.

Taip pat svarbu pažymėti, kad Lietuvos Aukščiausiasis Teismas yra konstatavęs, kad įstatyme nustatyta tokia mokėtojo paslaugų teikėjo atsakomybės už neautorizuotą mokėjimą sistema, pagal kurią mokėtojas turi teisę į neautorizuotos operacijos sumos sugrąžinimą, o mokėtojo paslaugos teikėjas turi pareigą ją sugrąžinti, išskyrus atvejus, jei nustatoma, kad: 1) mokėtojas veikia nesažiningai; 2) mokėtojas tyčia ar dėl didelio neatsargumo pažeidžia vieną ar kelias Mokėjimų įstatymo 34 straipsnyje nustatytas mokėtojo pareigas, susijusias su mokėjimo priemonėmis ir personalizuotais saugumo duomenimis. Nurodyta mokėtojo paslaugų teikėjo atsakomybės už neautorizuotą mokėjimą sistema reiškia griežtąją mokėtojo paslaugų teikėjo atsakomybę už atliktas neautorizuotas mokėjimo operacijas, t. y. atsakomybę be kaltės. Kita vertus, mokėtojo paslaugų teikėjo atsakomybė be kaltės neeliminuoja paties mokėtojo pareigos elgtis rūpestingai ir atsakingai. Todėl tuo atveju, jei mokėtojas elgiasi nesažiningai ar tyčia ar dėl didelio neatsargumo pažeidžia įstatyme jam nustatytas pareigas, paslaugos teikėjas yra atleidžiamas nuo atsakomybės. Ne bet kokių mokėtojo pareigų nevykdymas yra pagrindas atleisti mokėtojo paslaugos teikėją nuo atsakomybės, o būtent Mokėjimų įstatymo 34 straipsnyje nustatytų mokėtojo pareigų, kurios susijusios su mokėjimo priemonėmis ir personalizuotais saugumo duomenimis, be to, paprastas mokėtojo neatsargumas nėra laikomas mokėtojo paslaugos teikėjo atleidimo nuo atsakomybės sąlyga¹.

Duomenų, kad nagrinėjamu atveju pareiškėja galėjo veikti nesažiningai arba tyčia, nėra, todėl galimas mokėtojo sukčiavimas, kaip pagrindas atleisti mokėtojo mokėjimo paslaugų teikėją nuo pareigos atlyginti mokėtojai nuostolius dėl neautorizuotos mokėjimo operacijos įvykdymo, šiame sprendime atskirai nebus plačiau analizuojamas.

Taigi, sprendžiant, ar banko atsisakymas grąžinti pareiškėjai ginčijamos mokėjimo operacijos sumą laikytinas pagrįstu, būtina įvertinti, ar pareiškėjos elgesys, atskleidžiant tretiesiems asmenims personalizuotus saugumo duomenis, vertintinas kaip didelis neatsargumas, dėl kurio su mokėjimo operacijų įvykdymu atsiradę nuostoliai, kaip nustatyta Mokėjimų įstatymo 39 straipsnio 3 dalyje, tektų pačiai pareiškėjai.

Lietuvos Aukščiausiasis Teismas yra išaiškinęs, kad didelis neatsargumas pasireiškia neprotingu arba išskirtiniu rūpestingumo nebuvimu, kai asmuo nėra tiek rūpestingas, kiek akivaizdžiai būtina esamomis aplinkybėmis². Didelis mokėtojo neatsargumas gali būti konstatuojamas tik tuomet, jei mokėtojas elgėsi labai nerūpestingai. Kad mokėtojas elgėsi labai nerūpestingai, turi įrodyti mokėjimo paslaugų teikėjas, pateikdamas konkrečius tokį elgesį pagrindžiančius įrodymus. Ši įrodinėjimo našta negali būti perkelta mokėtojai³.

Dėl mokėtojo neatsargumo laipsnio vertinimo, pagrindinių jo kriterijų ir glaudaus ryšio su ginčo byloje nustatytų individualių specifinių aplinkybių visuma Lietuvos bankas yra ne kartą plačiau pasisakęs savo ginčų nagrinėjimo praktikoje⁴, todėl šiame sprendime bus pasisakoma tik šiais konkrečiais ginčo bylai aktualiais aspektais.

Neautorizuotos mokėjimo operacijos įvykdymo atveju didelis neatsargumas yra sietinas su vienos ar kelių Mokėjimų įstatymo 34 straipsnyje mokėtojai nustatytų pareigų, susijusių su mokėjimo priemone ir personalizuotais saugumo duomenimis, nevykdymu. Kaip yra konstatavęs Lietuvos Aukščiausiasis Teismas, neautorizuotos mokėjimo operacijos atveju mokėjimo paslaugų teikėjas turi įrodyti ne tik tai, kad mokėtojas pažeidė vieną ar kelias Mokėjimų įstatymo 34 straipsnyje nustatytas mokėtojo pareigas, susijusias su mokėjimo priemonėmis ir personalizuotais saugumo duomenimis, bet ir kad tai padarė dėl didelio

¹ Lietuvos Aukščiausiojo Teismo 2023 m. rugsėjo 12 d. nutartis civilinėje byloje Nr. e3K-3-182-1075/2023, 44 punktas.

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

³ Lietuvos Aukščiausiojo Teismo 2023 m. rugsėjo 12 d. nutartis civilinėje byloje Nr. e3K-3-182-1075/2023, 82 punktas.

⁴ Pavyzdžiui, ginčo bylos Nr. [2022-02496](#).

neatsargumo⁵.

Mokėjimų įstatymo 34 straipsnis nustato mokėtojo pareigą naudotis jam išduota mokėjimo priemone (nagrinėjamu atveju – mokėjimo kortele) pagal jos išdavimą ir naudojimą reglamentuojančias sąlygas, o sužinojus apie jos praradimą, vagystę arba neteisėtą pasisavinimą ar neautorizuotą jos naudojimą, nedelsiant apie tai pranešti mokėjimo paslaugų teikėjui arba jo nurodytam subjektui (Mokėjimų įstatymo 34 straipsnio 1 dalis), taip pat pareigą, gavus mokėjimo priemonę, imtis veiksmų, kad būtų apsaugoti personalizuoti saugumo duomenys (Mokėjimų įstatymo 34 straipsnio 2 dalis).

Bankas mano, kad nuostolius dėl ginčijamos mokėjimo operacijos pareiškėja patyrė dėl savo didelio neatsargumo, t. y. atskleisdama tretiesiems asmenims savo banko atpažinimo kodą, asmens kodą bei suveddama tik jai žinomus Smart-ID PIN1 ir PIN2 kodus ir taip suteikdama leidimą pareiškėjos vardu tretiesiems asmenims ne tik prisijungti prie pareiškėjos interneto banko, inicijuoti ginčijamą mokėjimo operaciją, bet ir pačiai pareiškėjai patvirtinant jos įvykdymą.

Banko sprendimas nekompensuoti pareiškėjos nuostolių dėl neautorizuotos ginčijamos mokėjimo operacijos įvykdymo galėtų būti vertinamas kaip pagrįstas tik tada, jeigu būtų įrodyta, kad pareiškėja, atskleisdama tam tikrus personalizuotus savo mokėjimo priemonių saugumo duomenis, leido inicijuoti, patvirtino ginčijamą mokėjimo operaciją, t. y. elgėsi itin aplaidžiai – buvo labai neatsargi.

Lietuvos bankas, siekdamas nustatyti, ar pareiškėjos elgesys šiuo atveju gali būti laikomas kaip labai neatsargus, vertino pareiškėjos elgesį pasitikint platformoje *skelbiu.lt* gautame pranešime nurodyta informacija ir spaudžiant pareiškėjai pateiktą aktyvią nuorodą, suvedant savo mokėjimo priemonės personalizuotus saugumo duomenis suklustotame *Omniva* interneto puslapyje bei patvirtinant atliekamus veiksmus naudojama atpažinties priemone – suvedant Smart -ID PIN1 ir PIN2 kodus, taip pat banko veiksmus, kurių jis prevenciškai ėmėsi ir imasi tam, kad padėtų susigrąžinti prarastas lėšas, supažindintų pareiškėją su sukčiavimo elektroninėje erdvėje rizikomis bei tapatybės patvirtinimo priemonės saugaus naudojimo, jos personalizuotų saugumo žymenų suvedimo ir atskleidimo reikšme bei teisinėmis pasekmėmis.

Vertinant pačios pareiškėjos elgesį, svarbu nustatyti, kaip pareiškėja, kaip mokėjimo paslaugų vartotoja, buvo įtikinta atskleisti savo mokėjimo priemonės personalizuotus saugos duomenis, įgalinusius trečiuosius asmenis inicijuoti ginčijamą mokėjimo operaciją.

Lietuvos bankas, įvertinęs pareiškėjos kreipimesi ir banko atsiliepime nurodytas aplinkybes bei kartu su kreipimusi ir atsiliepimu pateiktus duomenis, nustatė, kad prieš ginčijamos mokėjimo operacijos įvykdymą pareiškėja platformoje *skelbiu.lt* gavo tariamo pirkėjo siųstą pranešimą, kad šis ketina įsigyti pareiškėjos parduodamą prekę. Pareiškėja telefoninio pokalbio su banko darbuotoja metu, patvirtino, kad ji paspaudė trečiųjų asmenų jai atsiųstą aktyvią nuorodą bei tikslu į savo banko sąskaitą gauti pinigus už parduodamą prekę, suvedė savo personalizuotus saugos duomenis bei Smart-ID PIN1 bei PIN2 kodus.

Kaip jau buvo minėta pirmiau, Mokėjimų įstatymo 34 straipsnyje reglamentuojama viena iš mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigų – naudotis mokėjimo priemone pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas.

Banko ir pareiškėjos santykius reglamentuojančių banko Bendrųjų taisyklių (toliau – Taisyklės) 1 priedo 10 skyriuje nustatyta, 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. Taisyklių 11 skyriuje įvardijama PIN kodų suvedimo reikšmė mokėjimo operacijų vykdymo procese ir jų panaudojimo galimos pasekmės mokėtojui.

Banko ir pareiškėjos santykiams taip pat taikomas ir banko Paslaugų interneto banke teikimo sąlygų aprašas (toliau – Aprašas), kurio 21.4 papunktyje ir 39 punkte nurodyta, kad: „Klientas / naudotojas įsipareigoja saugoti atpažinimo priemones, nedelsdamas informuoti Banką apie šių priemonių praradimą ar slaptumo pažeidimą. Jei atpažinimo priemonių praradimas susijęs su trečiųjų asmenų neteisėtais veiksmais, tai klientas / naudotojas privalo apie tai nedelsdamas pranešti teisėsaugos institucijoms. Už atpažinimo priemonių saugumą ir tinkamą naudojimą, neatskleidimą tretiesiems asmenims yra atsakingas klientas; – Klientas / naudotojas įsipareigoja laikyti paslaptįje atpažinimo kodą, slaptažodžius, PIN kodus, neužrašyti jų ant generatoriaus ar kitų kartu su juo laikomų daiktų ir jokia kita forma neatskleisti ar

⁵ Lietuvos Aukščiausiojo Teismo 2023 m. rugsėjo 12 d. nutartis civilinėje byloje Nr. e3K-3-182-1075/2023, 78 punktas.

nepadaryti jų prieinamų tretiesiems asmenims.“

Taigi, pirmiau aptartos Taisyklių ir Aprašo nuostatos aiškiai ir nedviprasmiškai nustato tapatybės patvirtinimo priemonės personalizuotų saugumo duomenų naudojimo mokėjimo operacijų vykdymo procese paskirtį ir jų panaudojimo galimas pasekmes mokėtojui bei aiškiai ir nedviprasmiškai apibrėžia, kad už šių duomenų konfidencialumo išsaugojimą yra atsakingas mokėtojas, šiuo atveju – pareiškėja.

Atsižvelgiant į tai, manytina, kad pareiškėjos elgesys būtų laikomas kaip atitinkantis mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas, jei būtų nustatyta, kad pareiškėja ėmėsi pakankamų veiksmų (arba priešingai – nustačius, kad nuo tam tikrų veiksmų susilaikė) tam, kad jai banko išduotų mokėjimo priemonių personalizuotų saugumo duomenų, įgalinančių inicijuoti ir tvirtinti mokėjimus, konfidencialumas būtų tinkamai užtikrintas, o jai banko išduota mokėjimo priemonė būtų naudojama šalių sutartinius santykius reglamentuojančių dokumentų nustatyta tvarka bei sąlygomis.

Vertinant, ar pareiškėjos elgesys, kai ji paspaudė trečiųjų asmenų jai atsiųstą aktyvią nuorodą ir pateko į neva *Ominiva* interneto puslapį ir siekdama į savo sąskaitą gauti lėšas, suvedė savo banko atpažinimo kodą bei asmens kodą, gali būti vertinamas kaip labai neatsargus, t. y. toks elgesys, dėl kurio mokėjimo priemonės turėtojo veiksmai iš esmės skiriasi nuo atsargaus elgesio reikalavimų, pažymėtina, kad įprastai vien tik sukčių atsiųstos aktyvios nuorodos paspaudimas nėra laikomas itin neatsargiu mokėtojo elgesiu, nes dažnai sukčių suklastotos aktyvios nuorodos vizualiai būna gana panašios į tikrąsias interneto svetaines ir vartotojui, neturinčiam specialiųjų žinių, gali būti sudėtinga įvertinti atsiųstos nuorodos tikrumą.

Ginčo byloje nėra pateikta duomenų, kaip vizualiai atrodė trečiųjų asmenų suklastotas interneto puslapis, kuriame pareiškėja suvedė savo personalizuotus saugos duomenis, tačiau svarbu pažymėti, kad sukčiavimo ataka, į kurią pateko pareiškėja, yra ne nauja, gana plačiai visuomenėje žinoma, nes iš įvairių informacijos šaltinių periodiškai skelbiama nemažai informacijos ir vartotojai raginami būti budriais bei nespausti aktyvių nuorodų. Atsižvelgiant į pirmiau minėtą, galima teigti, kad pareiškėjai galėjo kilti įtarimų dėl aktyvios nuorodos gavimo ir pareiškėja, jeigu tik būtų neskubėjusi vykdyti trečiųjų asmenų nurodymų bei gautą informaciją vertinusi kritiškai, būtų galėjusi suprasti ar bent įtarti, kad prieš ją gali būti vykdoma sukčiavimo ataka.

Vertinant, ar pareiškėjos elgesys, kai ji paspaudė aktyvią nuorodą ir pateko į suklastotą *Omniva* interneto svetainę, norėdama gauti pinigines lėšas į savo banko sąskaitą, suvedė savo banko atpažinimo kodą, asmens kodą bei Smart-ID PIN1 kodą, taip patvirtindama leidimą tretiesiems asmenims pareiškėjos vardu prisijungti prie jos interneto banko bei inicijuoti ginčijamą mokėjimo operaciją bei vėliau jos įvykdymą patvirtindama suvedant Smart-ID PIN2 kodą, gali būti vertinamas kaip labai neatsargus, t. y. toks elgesys, dėl kurio mokėjimo priemonės turėtojo veiksmai iš esmės skiriasi nuo atsargaus elgesio reikalavimų, pažymėtina, kad be to, jog sukčiavimo ataka nebuvo nauja, pats bankas savo paslaugų vartotojus informuoja apie dažniausiai pasitaikančias sukčiavimo atakas. Minėtą informaciją bankas skelbia tiek savo interneto banko puslapyje, tiek socialiniuose tinkluose, tiek ir asmeniškai vartotojams siųsdamas pranešimus. Banko Lietuvos bankui pateiktais duomenimis, bankas pareiškėją apie sukčiavimo grėsmes ir elektroninėje erdvėje kylančias rizikas naudojantis mokėjimo paslaugomis pareiškėją informavo asmeniškai siųstais pranešimais⁶.

Banko pateiktais duomenimis, pareiškėja Smart-ID naudojosi nuo 2018 m., ja naudodamasi tvirtino mokėjimo operacijas, taigi, turėjo patirties ir suprato, kad PIN kodų slaptažodžiais gali būti tvirtinama mokėjimo operacija. Iš ginčo bylos duomenų matyti, kad pareiškėja buvo patyrusi Smart-ID, kaip tapatybės patvirtinimo priemonės, naudotoja ir galėjo suprasti savo veiksmų su mokėjimo priemone rizikas ir galimas pasekmes.

Vertinant pareiškėjos veiksmus paspaudus jai trečiųjų asmenų pateiktą aktyvią nuorodą, patekus į suklastotą *Omniva* interneto svetainę ir suvedus savo banko atpažinimo kodą bei asmens kodą, svarbu tai, kad pareiškėja tikėjosi parduoti prekę ir už ją į savo sąskaitą gauti pinigines lėšas. Tai reiškia, kad pareiškėja neturėjo tikslo iš savo sąskaitos panaudojant savo mokėjimo priemonės duomenis įvykdyti mokėjimo operaciją. Būtent siekdama už prekę gauti pinigus į savo banko sąskaitą pareiškėja suvedė savo personalizuotus saugos duomenis ir pavertino lėšų įskaitymą į banko sąskaitą. Taigi, tam, kad pareiškėja į savo banko sąskaitą gautų

⁶ 2024 m. gegužės 1d. 7, 2024 m. rugpjūčio 14 d., 2024 m. spalio 8 d., 2024 m. lapkričio 19 d., 2025 m. vasario 14 d.

pinigines lėšas, jos buvo prašoma suvesti personalizuotus duomenis, kurie įprastai suvedami norint inicijuoti ir patvirtinti mokėjimo operaciją iš banko sąskaitos.

Kad pinigines lėšas būtų gautos į banko sąskaitą, bankai neprašo sąskaitos turėtojo suvesti savo banko atpažinimo kodo, asmens kodo bei suvesti Smart-ID PIN1 ir PIN2 kodų. Pareiškėjai faktas, kad norėdama į savo sąskaitą gauti pinigines lėšas ji turėjo suvesti duomenis, kurie iš esmės yra reikalingi atlikti priešingą veiksmą – patvirtinti lėšų iš banko sąskaitos nurašymą, nesukėlė įtarimų ir pareiškėja vykdė trečiųjų asmenų nurodymus.

Svarbu pažymėti, kad pareiškėja telefoninio pokalbio su banko darbuotoja metu, banko darbuotojai paaiškino, kad su ja susiekęs tariamas pirkėjas jai nurodė, kad lėšų suma, kurios įskaitymą pareiškėja turinti patvirtinti mokėjimo nurodyme bus nurodyta fiktyvi t. y. ne tokia pati, kokia buvo pareiškėjos parduodamos prekės kaina (150 Eur), tačiau pareiškėjai ir informacija, kad mokėjimo nurodyme bus pateikta kita suma nei parduodama prekė nesukėlė įtarimų.

Taigi, pareiškėja, nors ir turėjo galimybę kritiškai įvertinti savo veiksmų su mokėjimo priemone riziką ir galimas pasekmes ir turėjo galimybę susilaikyti nuo tolimesnių veiksmų, tačiau nuo jų nesusilaikė, priešingai, vykdė trečiųjų asmenų nurodymus ir suvedė savo Smart-ID PIN1 ir PIN2 kodus.

Kaip minėta, bankas, prieš pareiškėjai suvedant Smart-ID PIN1 ir PIN2 kodus, rodė informaciją, koku tikslu yra prašoma suvesti minėtus kodus. Tačiau, nepaisydama banko jai teikiamos informacijos, pareiškėja toliau tęsė veiksmus su savo mokėjimo priemone ir taip tretiesiems asmenims suteikė galimybę jos vardu prisijungti prie banko sąskaitos, inicijuoti ginčijamą mokėjimo operaciją, kurios įvykdymą patvirtino pati pareiškėja.

Įvertinus pirmiau nurodytas aplinkybes, Lietuvos banko nuomone, galima daryti išvadą, kad, jeigu pareiškėja būtų buvusi pakankamai kritiška savo su mokėjimo priemone atliekamų veiksmų atžvilgiu ir būtų susilaikiusi nuo veiksmų su savo mokėjimo priemone, ji būtų galėjusi išvengti neautorizuotos mokėjimo operacijos iš savo sąskaitos įvykdymo. Pareiškėja turėjo galimybę suprasti, kad jos prašoma atlikti veiksmus, kurių nėra įprastai prašoma atlikti norint pinigines lėšas gauti į savo sąskaitą, o priešingai – yra prašoma atlikti veiksmus, kurie įprastai yra atliekami norint įvykdyti mokėjimo operacijas iš banko sąskaitos. Pareiškėja turėjo kritiškai įvertinti trečiųjų asmenų prašomus atlikti veiksmus su savo mokėjimo priemone.

Vis dėlto pareiškėja faktą, kad jos buvo prašoma suvesti Smart-ID PIN1 ir PIN2 kodus nevertino kritiškai, nepaisė banko jai pateiktos informacijos, vykdė trečiųjų asmenų jai pateiktus nurodymus. Iš ginčo byloje surinktų duomenų, galima daryti išvadą, kad pareiškėja mokėjimo priemone naudojos nesilaikydama mokėjimo priemonės išdavimą ir naudojimą reglamentuojančių sąlygų ir neįvykdė Mokėjimų įstatymo 34 straipsnyje reglamentuojamų mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigų.

Lietuvos banko vertinimu, toks pareiškėjos elgesys gali būti pripažintas kaip elgesys, iš esmės besiskiriantis nuo atsargaus elgesio reikalavimų, tai galiausiai ir lėmė, kad pareiškėja prarado savo mokėjimo priemonę, o tretieji asmenys įgijo galimybę pareiškėjos vardu inicijuoti ginčijamą mokėjimo operaciją.

Mokėjimų įstatymo 39 straipsnio 3 dalyje nustatyta, kad mokėtojai tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai, jeigu jis juos patyrė veikdamas nesažiningai arba tyčia ar dėl didelio neatsargumo neįvykdęs vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų.

Įvertinus pirmiau išdėstytą informaciją, konstatuotina, kad yra pagrindas pareiškėjai taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, todėl šiuo pagrindu pareiškėjos reikalavimas bankui grąžinti neautorizuotos ginčijamos mokėjimo operacijos lėšų sumą yra nepagrįstas ir atmetinas.

2. Dėl mokėjimo nurodymo įvykdyti ginčijamą mokėjimo operaciją atšaukimo

Pareiškėja teigė, kad bankas turėjo nevykdyti ir atšaukti ginčijamą mokėjimo operaciją, nes pokalbio su banko darbuotoju metu pareiškėja banką informavo, kad mokėjimo operacijos pati neinicijavo ir lėšos pareiškėjos banko sąskaitoje dar buvo tik rezervuotos.

Vertinant banko pareigą atšaukti ginčijamos mokėjimo operacijos vykdymą, pažymėtina, kad, pagal Mokėjimų įstatymo 44 straipsnio 1 dalies nuostatas, mokėjimo paslaugų vartotojas negali atšaukti mokėjimo nurodymo po to, kai ji gauna mokėtojo mokėjimo paslaugų teikėjas, išskyrus šiame straipsnyje nustatytas išimtis. Minėto Mokėjimų įstatymo straipsnio 4 dalyje taip pat nustatyta, kad, pasibaigus 1 dalyje nurodytam laikotarpiui, mokėjimo

nurodymas gali būti atšauktas tik tuo atveju, kai dėl to susitaria mokėjimo paslaugų vartotojas ir atitinkamas mokėjimo paslaugų teikėjas, o šio straipsnio 2 dalyje numatytais atvejais būtinas ir gavėjo sutikimas.

Taigi, pasibaigus Mokėjimų įstatymo 44 straipsnio 1 dalyje nurodytam terminui, mokėjimo nurodymas gali būti atšauktas tik dėl to susitarus vartotojui ir jo mokėjimo paslaugų teikėjui, todėl nurodytos galimybės (t. y. mokėjimo nurodymo atšaukimo) įtvirtinimas Mokėjimų įstatyme neturėtų būti vertinamas kaip priverstinis lėšų gražinimas mokėtojui, esant jo atitinkamam prašymui (pasibaigus 44 straipsnio 1 dalyje nurodytam terminui).

Taisyklių 3.3. punktas nustato, kad „sutikimą atlikti mokėjimo operaciją galite atšaukti iki mokėjimo nurodymo gavimo banke momento. Mokėjimo nurodymo įvykdymo trukmę skaičiuojame nuo to momento, kai mokėjimo nurodymą laikome gautu banke“. Taisyklių 4.2 punkte reglamentuojama, kad mokėjimo nurodymas laikomas gautu: „mokėjimo nurodymo pateikimo dieną, jeigu jį pateikėte banko darbo dieną iki kainyne nurodyto laiko (Taisyklių 4.2.1. papunktis); pirmą banko darbo dieną po mokėjimo nurodymo pateikimo dienos, jeigu jį pateikėte po kainyne nurodyto laiko (Taisyklių 4.2.2. papunktis); kai tik jį pateikiate bankui, nepriklausomai nuo dienos ir valandos, jeigu tai yra momentinis mokėjimas arba mokėjimas į kitą sąskaitą, esančią (SEB) Banke (Taisyklių 4.2.3 papunktis)“.

Pažymėtina, kad nei Mokėjimų įstatyme, nei šalių susitarime (banko mokėjimo paslaugų teikimo sąlygose) nurodytos sąlygos atšaukti mokėjimo nurodymus įvykdyti ginčijamas mokėjimo operacijas nagrinėjamo ginčo atveju nebuvo nustatytos. Pareiškėja į banką kreipėsi kelios minutės po to, kai buvo inicijuota ir patvirtinta ginčijama mokėjimo operacija, o banko darbuotoja iš karto, nedelsdama blokavo prieigą prie pareiškėjos interneto banko bei iš karto, telefoninio pokalbio su pareiškėja metu, pateikė prašymą atšaukti ginčijamos mokėjimo operacijos įvykdymą.

Lietuvos banko vertinimu, banko veiksmai, kurių jis ėmėsi tam, kad pareiškėjos interneto banko paskyra būtų blokuota per kaip įmanomai trumpiausią laiką nuo pranešimo bankui apie neautorizuotos mokėjimo operacijos įvykdymą, kad būtų išvengta dar didesnių nuostolių bei banko veiksmai, kurių jis ėmėsi, kad ginčijama mokėjimo operacija būtų atšaukta, atitinka Lietuvos banko Sukčiavimo prevencijos gairėse bankams pateikiamas rekomendacijas, per kiek įmanoma trumpiausią laiką nuo pranešimo apie neautorizuotas mokėjimo operacijas gavimo momento imtis veiksmų apriboti naudojimąsi mokėjimo priemone bei atšaukti mokėjimo operacijos įvykdymą.

Pagal Mokėjimų įstatymo 46 straipsnį, mokėjimo paslaugų teikėjas privalo užtikrinti, kad po mokėjimo nurodymo gavimo mokėjimo operacijos suma būtų įskaityta į mokėjimo nurodyme nurodyto gavėjo sąskaitą minėtame straipsnyje nustatytais terminais, o Mokėjimų įstatymo 51 straipsnio 4 dalyje nustatyta mokėjimo paslaugų teikėjo atsakomybė už mokėtojo inicijuotos mokėjimo operacijos neįvykdymą, netinkamą ar pavėluotą įvykdymą. Aplinkybė, kad pareiškėjos ginčijama mokėjimo operacija iš tiesų yra neautorizuota, nors ir atitiko pareiškėjos ir banko sutartą sutikimo atlikti mokėjimo operaciją davimo tvarką, paaiškėjo vėliau, nei ši ginčijama mokėjimo operacija buvo patvirtinta ir įvykdyta. Tai reiškia, kad šiuo atveju bankas neturėjo teisės aktuose nustatyto pagrindo tokio mokėjimo nurodymo nevykdyti ar jį atšaukti.

Remiantis ginčo byloje esančiais duomenimis, pareiškėjos prašymas atšaukti ginčijamą mokėjimo operaciją bankui buvo pateiktas po to, kai mokėjimo nurodymą jau buvo gavęs bankas, todėl Mokėjimų įstatyme nustatytas mokėjimų nurodymų atšaukimo terminas jau buvo praėjęs ir bankas atšaukti pareiškėjos vardu pateikto mokėjimo nurodymo nebegalėjo.

Be to, ginčo byloje pateiktais duomenimis, bankas inicijavo ginčijamos mokėjimo operacijos atšaukimą, tačiau lėšų sugrąžinti nepavyko.

Atsižvelgiant į tai, kas buvo išdėstyta pirmiau, nėra pagrindo vertinti, kad bankas nepagrįstai įvykdė ginčijamą mokėjimo operaciją ir kad nepagrįstai jos neatšaukė.

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 tapataus ginčo dalyko kreiptis į teismą 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