



**LIETUVOS BANKO
TEISĖS IR LICENCIJAVIMO DEPARTAMENTO
DIREKTORIUS**

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

2026-01-29 Nr. 429-27
Vilnius

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

N u s t a t y t a:

2025 m. birželio 11 d. iš pareiškėjo banko sąskaitos, panaudojant tik pareiškėjui žinomus personalizuotus saugos duomenis, lėšų gavėjui *duomenys neskelbiami* (toliau – lėšų gavėjas) buvo atlikta 2 700 Eur mokėjimo operacija (toliau – ginčijama mokėjimo operacija).

Ginčo byloje nustatyta, kad pareiškėjas, turėdamas tikslą prisijungti prie UAB „Elektrum Lietuva“ interneto svetainės, *Google* paieškos sistemoje suvedė reikšminius žodžius *Elektrum*, pateko į minėtos bendrovės suklastotą puslapį ir paspaudė banko logotipą. Paspaudęs aktyvią nuorodą, pareiškėjas buvo nukreiptas į suklastotą banko interneto banko puslapį, kuriame buvo prašoma įvesti tik pareiškėjui žinomus personalizuotus saugos duomenis, reikalingus prisijungti prie interneto banko, – interneto banko atpažinimo ir asmens kodus. Taip pat pareiškėjas prisijungimą turėjo patvirtinti jo naudojamos atpažinimo priemonės „Smart-ID“ paskyros PIN1 kodu. Pareiškėjui suvedus šiuos duomenis, tretieji asmenys įgijo galimybę prisijungti prie pareiškėjo banko sąskaitos ir inicijuoti ginčijamą mokėjimo operaciją. Ginčijamos mokėjimo operacijos įvykdymas buvo patvirtintas tik vienam pareiškėjui žinomam „Smart-ID“ PIN2 kodu.

Remdamasis visa surinkta informacija, bankas priėmė sprendimą atsisakyti pareiškėjui atlyginti jo patirtus nuostolius, nes nustatė, kad ginčijama mokėjimo operacija buvo įvykdyta dėl pareiškėjo itin neatsargių veiksmų. Banko nuomone, tai ir lėmė, kad pareiškėjas patyrė nuostolių. Pareiškėjas su tuo nesutiko, todėl tarp šalių kilo ginčas.

Kreipimesi į Lietuvos banką pareiškėjas prašo įpareigoti banką grąžinti ginčijamos mokėjimo operacijos metu iš jo banko sąskaitos nurašytas lėšas, t. y. grąžinti 2 700 Eur. Pareiškėjas Lietuvos bankui paaiškino, kad „be mano žinios bankas tvarkė mano sąskaitą, 2025-06-11 buvo atliktas 2 700,00 Eur pavedimas kažkokiam man nežinomam asmeniui, tuo metu, kai aš miegojau. Apie aplaidų banko atliktą pavedimą iš mano sąskaitos ir lėšų nurašymo faktą pamačiau tik ryte. Pavedimas neaiškiam asmeniui į užsienio sąskaitą buvo atliktas banko momentaliai net neįsitikinęs, ar tai aš jį atlieku, ir ar esu tikras dėl tokio veiksmo. Suma buvo didelė, ir bankas tokio pavedimo neblokavo???!“ Papildomai telefonu pareiškėjas Lietuvos bankui teigė, kad dieną prieš ginčijamos mokėjimo operacijos įvykdymą jis per *Google* paieškos sistemą jungėsi prie *Elektrum* ir tuo tikslu suvedė „Smart-ID“ paskyros PIN1 ir PIN2 kodus. Pareiškėjas paaiškino, kad prieš suveddamas „Smart-ID“ paskyros PIN2 nematė banko rodomos informacijos nei apie ginčijamos mokėjimo operacijos sumą, nei apie gavėją. Pareiškėjo nuomone, bankas neužtikrino lėšų jo banko sąskaitoje saugumo, nevykdė mokėjimo operacijų stebėsenos.

Atsiliepime į pareiškėjo kreipimąsi bankas nurodo nesutinkąs su pareiškėjo reikalavimu ir prašo jį atmesti. Banko teigimu, pareiškėjo veiksmai su savo mokėjimo priemone gali būti vertinami kaip labai neatsargūs, nes pareiškėjas, prieš suveddamas „Smart-ID“ PIN1 ir PIN2 kodus, nekreipė dėmesio į banko jam rodomą informaciją.

Bankas paaiškino, kad, jo turimais sistemų duomenimis, pareiškėjas, prieš suveddamas „Smart-ID“ PIN1 kodą, turėjo galimybę matyti, kad tvirtina prisijungimą prie banko interneto

banko, nes jo telefone atsidariusiame „Smart-ID“ programėlės ekrane buvo pateiktas tokio turinio teksto pranešimas: „Jungiatės prie SEB interneto banko.“

Banko turimų sistemų duomenimis, tretieji asmenys prisijungė prie pareiškėjo interneto banko ir inicijavo ginčijamos mokėjimo operacijos įvykdymą, o sutikimą įvykdyti šią mokėjimo operaciją davė pats pareiškėjas, suveddamas „Smart-ID“ PIN2 kodą. Bankas, prieš pareiškėjui vedant „Smart-ID“ PIN2 kodą, jo mobiliojo telefono ekrane rodė tiek ginčijamos mokėjimo operacijos sumą, tiek ir gavėjo duomenis: „2 700,00 EUR i saskaita ***6803.“

Banko teigimu, pareiškėjas turėjo visas galimybes perskaityti informaciją apie veiksmą, kuriam jo prašoma duoti sutikimą, ir susilaikyti nuo tolimesnių veiksmų, tačiau jis pasirinko suvesti „Smart-ID“ PIN2 kodą.

Banko vertinimu, tai, kad pareiškėjas, veddamas savo personalizuotus saugos duomenis, įskaitant ir „Smart-ID“ PIN2 kodą, nors jam aiškiai buvo rodoma vedamo kodo paskirtis, kritiškai nevertino savo atliekamų veiksmų, rodo, jog jis dėl didelio neatsargumo neišsaugojo savo personalizuotų saugos duomenų, dėl to tretieji asmenys jais galėjo pasinaudoti ir be pareiškėjo žinios inicijuoti ginčijamą mokėjimo operaciją.

Bankas pažymėjo, kad iki ginčijamos mokėjimo operacijos įvykdymo bankas pareiškėją buvo informavęs apie sukčiavimo grėsmes naudojantis mokėjimo paslaugomis¹. Bankas teigia savo klientus nuolat informuojantis apie sukčiavimo pavojus ir rizikas, susijusias su sukčiavimais elektroninėje erdvėje, ir primena, kokie ir kaip vartotojų duomenys turėtų būti saugomi ir neatskleisti tretiesiems asmenims.

Papildomai bankas pažymėjo, kad, gavęs pareiškėjo pretenziją dėl neautorizuotos mokėjimo operacijos įvykdymo, nedelsdamas kreipėsi į lėšų gavėją, tačiau lėšų sugrąžinti nepavyko.

Atsižvelgdamas į visas pirmiau nurodytas aplinkybes, bankas prašė atmesti pareiškėjo reikalavimą kaip nepagrįstą.

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

Vadovaujantis Lietuvos banko valdybos 2012 m. sausio 26 d. nutarimu Nr. 03-23 patvirtintų Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių 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. Lietuvos bankas ginčo nagrinėjimo proceso metu neatlieka Lietuvos Respublikos Lietuvos banko įstatymo 42¹ straipsnyje reglamentuotų patikrinimų, skirtų faktinėms aplinkybėms, susijusioms su Lietuvos banko prižiūrimo finansų rinkos dalyvio galimu Lietuvos banko kompetencijai priskirtų teisės aktų reikalavimų pažeidimu, nustatyti ir įvertinti. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Pareiškėjo ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjui ginčijamos mokėjimo operacijos metu iš jo sąskaitos banke pervestą sumą. Pareiškėjas neigia autorizavęs ginčijamą mokėjimo operaciją ir teigia, kad bankas jam nepateikė informacijos apie mokėjimo operacijos sumą bei gavėją, taip pat kad neapsaugojo lėšų jo banko sąskaitoje. Banko teigimu, pareiškėjo veiksams būdingas didelis neatsargumas, todėl bankas negali būti įpareigotas jam 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).

Pareiškėjo nurodytos aplinkybės, kad ginčijama mokėjimo operacija nėra jo autorizuota, o pareiškėjo personalizuotus saugumo duomenis tretieji asmenys gavo apgaulės būdu, bankas atsiliepime neginčija. Priešingai, bankas savo paaiškinimuose nurodo, kad dėl pareiškėjo

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

atskleistų duomenų tretieji asmenys įgijo galimybę inicijuoti ginčijamą mokėjimo operaciją. Dėl šios priežasties yra akivaizdu, kad ginčijamos mokėjimo operacijos inicijavimas ir patvirtinimas neatitiko paties pareiškėjo valios, nors formaliai (pagal išorinius požymius) ir sutapo su pareiškėjo ir banko sutarta sutikimo atlikti mokėjimo operaciją davimo forma ir tvarka. Atsižvelgdamas į tai, Lietuvos bankas daro išvadą, kad ginčijama mokėjimo operacija, atlikta nesant pareiškėjo valios ir neišreiškus valinių veiksmų patvirtinti ginčijamą mokėjimo operaciją, laikytina neautorizuota.

Siekdamas išspręsti tarp šalių kilusį ginčą ir įvertinti pareiškėjo bankui keliamo reikalavimo pagrįstumą, Lietuvos bankas vertins, ar: 1) bankas, atsisakydamas grąžinti pareiškėjui ginčijamos mokėjimo operacijos metu pervestas lėšas, pagrįstai rėmėsi Mokėjimų įstatymo 39 straipsnio 3 dalimi; 2) ar bankas užtikrino lėšų pareiškėjo banko sąskaitoje saugumą.

1. Dėl banko pareigos pareiškėjui grąžinti ginčijamos mokėjimo operacijos sumą.

Mokėjimų įstatymo 39 straipsnio 3 dalyje nustatyta, kad mokėtojai 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.

Taip pat svarbu pažymėti, kad Lietuvos Aukščiausiasis Teismas yra konstatavęs, jog 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 nesąžiningai; 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, kai mokėtojas elgiasi nesąžiningai arba 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 sąlyga².

Duomenų, kad nagrinėjamu atveju pareiškėjas galėjo veikti nesąžiningai 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 pareiškėjui ginčijamos mokėjimo operacijos sumą laikytinas pagrįstu, būtina įvertinti, ar pareiškėjo elgesys, atskleidžiant tretiesiems asmenims personalizuotus saugumo duomenis, vertintinas kaip didelis neatsargumas, dėl kurio su mokėjimo operacijos įvykdymu atsiradę nuostoliai, kaip nustatyta Mokėjimų įstatymo 39 straipsnio 3 dalyje, tektų pačiam pareiškėjui.

Lietuvos Aukščiausiasis Teismas yra išaiškinęs, kad didelis neatsargumas pasireiškia neprotingu arba išskirtiniu rūpestingumo nebuvimu, kai asmuo nėra tiek rūpestingas, kiek akivaizdžiai būtina esamomis aplinkybėmis³. 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 mokėtojui⁴.

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 praktikoje⁵, todėl šiame sprendime bus pasisakoma tik šiai konkrečiai ginčo bylai aktualiais aspektais.

Neautorizuotos mokėjimo operacijos įvykdymo atveju didelis neatsargumas yra sietinas

² Lietuvos Aukščiausiojo Teismo 2023 m. rugsėjo 12 d. nutartis civilinėje byloje Nr. e3K-3-182-1075/2023, 44 punktas.

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

⁴ Lietuvos Aukščiausiojo Teismo 2023 m. rugsėjo 12 d. nutartis civilinėje byloje Nr. e3K-3-182-1075/2023, 82 punktas.

⁵ Pavyzdžiui, ginčo byla Nr. 2022-02496.

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 tai, kad tai padarė dėl didelio neatsargumo⁶.

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 pareiškėjas patyrė dėl savo didelio neatsargumo, t. y. pareiškėjas, perduodamas tretiesiems asmenims savo prisijungimo prie interneto banko duomenis (banko atpažinimo ir asmens kodus), prisijungimą prie interneto banko patvirtindamas „Smart-ID“ programėlės PIN1 kodu, suteikė leidimą tretiesiems asmenims iš jo banko sąskaitos inicijuoti ginčijamą mokėjimo operaciją, kurią pareiškėjas pats patvirtino, suveddamas „Smart-ID“ programėlės PIN2 kodą.

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

Lietuvos bankas, siekdamas nustatyti, ar pareiškėjo elgesys šiuo atveju gali būti laikomas labai neatsargiu, vertino jo elgesį jungiantis prie UAB „Elektrum Lietuva“ svetainės, suvedant savo mokėjimo priemonės personalizuotus saugumo duomenis suklustotame interneto banko puslapyje bei patvirtinant atliekamus veiksmus naudojama atpažinties priemone – suvedant „Smart-ID“ programėlės PIN1 ir PIN2 kodus, taip pat banko veiksmus, kurių jis prevenciškai ėmėsi ir imasi tam, kad 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 paties pareiškėjo elgesį, svarbu nustatyti, kaip pareiškėjas, kaip mokėjimo paslaugų vartotojas, buvo įtikintas atskleisti savo mokėjimo priemonės personalizuotus saugos duomenis, įgalinusius trečiuosius asmenis inicijuoti ginčijamą mokėjimo operaciją.

Lietuvos bankas, įvertinęs pareiškėjo kreipimesi ir banko atsiliepime nurodytas aplinkybes bei kartu su kreipimusi ir atsiliepimu pateiktus duomenis, nustatė, kad prieš ginčijamos mokėjimo operacijos įvykdymą pareiškėjas savo iniciatyva jungėsi prie galimai suklustotos UAB „Elektrum Lietuva“ interneto svetainės, prisijungęs paspaudė banko logotipą, pateko į suklustotą banko interneto banko puslapį, jame suvedė prašomus nurodyti duomenis: banko atpažinimo ir asmens kodus. Šie duomenys, kaip paaiškėjo vėliau, buvo nusavinti trečiųjų asmenų (sukčių) ir panaudoti tam, kad būtų prisijungta prie pareiškėjo interneto banko paskyros ir inicijuota ginčijama mokėjimo operacija. Trečiųjų asmenų prisijungimas prie pareiškėjo interneto banko paskyros buvo patvirtintas pačiam pareiškėjui suvedus „Smart-ID“ programėlės PIN1 kodą bei vėliau ginčijamą mokėjimo operaciją patvirtintus, suvedant „Smart-ID“ programėlės PIN2 kodą.

Kaip pirmiau minėta, Mokėjimų įstatymo 34 straipsnyje reglamentuojama viena iš mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigų – naudotis mokėjimo priemone pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas. To paties straipsnio 2 dalyje nurodyta, kad mokėjimo paslaugų vartotojas, gavęs mokėjimo priemonę, privalo imtis veiksmų, kad būtų apsaugoti personalizuoti saugumo duomenys.

Banko ir pareiškėjo santykius reglamentuojančių banko Bendrųjų paslaugų teikimo taisyklių (toliau – Taisyklės) Taisyklių 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

⁶ Lietuvos Aukščiausiojo Teismo 2023 m. rugsėjo 12 d. nutartis civilinėje byloje Nr. e3K-3-182-1075/2023, 78 punktas.

jokiems kitiems asmenims.

Taisyklių 11 skyriuje įvardinta PIN kodų suvedimo reikšmė mokėjimo operacijų vykdymo procese ir jų panaudojimo galimos pasekmės klientui⁷. Banko pateiktais duomenimis, pareiškėjas su Taisyklėmis ir jų naujausiais pakeitimais buvo asmeniškai supažindintas 2024 m. sausio 17 d., todėl pareiškėjas turėjo žinoti ir suprasti, kaip svarbu atidžiai ir apdairiai elgtis vedant PIN kodus.

Banko Paslaugų interneto banke teikimo sąlygų aprašo (toliau – Aprašas), kuris taip pat taikomas banko ir pareiškėjo santykiams, 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 privalo apie tai nedelsdamas pranešti teisėsaugos institucijoms. Už atpažinimo priemonių saugojimą ir tinkamą naudojimą, neatskleidimą tretiesiems asmenims yra atsakingas klientas.“

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

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

Vertinant, ar pareiškėjo elgesys, kai jis suklustotoje UAB „Elektrum Lietuva“ svetainėje paspaudė nuorodą į suklustotą banko interneto banko puslapį ir suvedė savo banko atpažinimo ir asmens kodus bei savo mobiliajame telefone suvedė „Smart-ID“ programėlės PIN1 kodą, taip patvirtindamas trečiųjų asmenų prisijungimą prie savo interneto banko paskyros, o vėliau savo mobiliajame telefone suvedė „Smart-ID“ programėlės PIN2 kodą, taip patvirtindamas ginčijamos mokėjimo operacijos įvykdymą, 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 panašaus pobūdžio ginčo bylose Lietuvos bankas vertina, kad vien tik faktas, jog mokėtojas paspaudžia jam trečiųjų asmenų atsiųstą aktyvią nuorodą ir nepastebi, kad patenka į suklustotą kokios nors bendrovės interneto puslapį, savaime nereiškia mokėtojo didelio neatsargumo. Paprastai sukčių pateiktos tiek pačios nuorodos į suklustotas bendrovių interneto svetaines, tiek ir pačios svetainės būna parengtos labai profesionaliai, dėl to vidutiniam vartotojui pagrįstai gali atrodyti, kad jis jungiasi prie tikros kokios nors bendrovės interneto svetainės.

Nagrinėjamo ginčo atveju iš pareiškėjo ir banko Lietuvos bankui pateiktų paaiškinimų galima teigti, kad sukčiavimo ataka, nukreipta prieš pareiškėją, buvo gerai parengta ir pareiškėjui, kaip vidutiniam vartotojui, pagrįstai galėjo atrodyti, kad suklustotoje UAB „Elektrum Lietuva“ svetainėje, paspausdamas banko logotipą, jis jungiasi prie savo interneto banko.

Banko Lietuvos bankui pateikti duomenys patvirtina, kad bankas, prieš pareiškėjui suvedant „Smart-ID“ programėlės PIN1 kodą, rodė pranešimą „Jungiatės prie SEB interneto banko“. Taigi, pareiškėjui pagrįstai galėjo atrodyti, kad, suveddamas „Smart-ID“ programėlės PIN1 kodą, jis jungiasi prie savo interneto banko.

Tačiau atkreiptinas dėmesys, kad panašaus pobūdžio sukčiavimo atakos nėra naujos ir visuomenėje gana plačiai žinomos, nes periodiškai skelbiama nemažai viešai prieinamos informacijos, įspėjančios vartotojus apie panašias sukčiavimo atkas ir raginančios juos būti budrius naudojant savo personalizuotus saugos duomenis.

Banko Lietuvos bankui pateiktais duomenimis, bankas pareiškėją asmeniškai jam siųstais

⁷ „Smart-ID“, SEB mobiliosios programėlės ar slaptažodžių generatoriaus PIN1, PIN2 kodus ir mobiliojo parašo „Mobile-ID“ sPIN1, sPIN2 kodus, naudojate: - PIN1, sPIN1 kodą – jūsų tapatybei patvirtinti, kai jungiatės prie atitinkamos paskyros, pvz., SEB interneto banko ir SEB mobiliojoje programėlės, SEB mobiliojoje programėlėje, susiedami mokėjimo kortelę su „Google Pay“, „Apple Pay“, kita skaitmenine pinigine ir mobiliaisiais įrenginiais, tvirtindami mokėjimą kortele 3D būdu – PIN2, sPIN2 kodą – pasirašydami elektroniniu parašu, tvirtindami operacijas, kitus veiksmus ir elektroninius dokumentus – mokėjimo pavedimus, sutartis, jų pakeitimus ir kt.“

elektroniniais laiškais informavo apie būdus, kuriais sukčiai gali mėginti pasisavinti iš banko sąskaitos pinigines lėšas, atkreipė pareiškėjo dėmesį į personalizuotų saugos duomenų mokėjimo operacijų vykdymo procese paskirtį ir galimas neatsargaus naudojimo pasekmes.

Taigi, iš šių duomenų matyti, kad bankas prevenciškai dėjo pastangas tam, kad pareiškėjas būtų supažindintas su sukčiavimo elektroninėje erdvėje rizikomis bei tapatybės patvirtinimo priemonės saugaus naudojimo, jos personalizuotų saugumo žymenų suvedimo ir atskleidimo reikšme bei teisinėmis pasekmėmis.

Vertinant tolesnius pareiškėjo veiksmus paspaudus aktyvią nuorodą ir patekus į trečiųjų asmenų suklastotą banko interneto banko puslapį, svarbu tai, kad pareiškėjas tikėjosi, kaip jis pats paaiškino, prisijungti prie UAB „Elektrum Lietuva“ svetainės.

Nors pareiškėjas teigia, kad bankas jam, prieš suvedant „Smart-ID“ programėlės PIN2 kodą, nerodė informacijos nei apie sumą, nei apie gavėją, tačiau banko Lietuvos bankui pateikti duomenys įrodo, kad prieš ginčijamos mokėjimo operacijos įvykdymą bankas pareiškėjui rodė tiek mokėjimo operacijos sumą, tiek ir lėšų gavėjos duomenis: „2 700,00 EUR i sąskaita ***6803.“

Iš banko prieš mokėjimo operacijos įvykdymo patvirtinimą pareiškėjui pateiktos informacijos galima teigti, kad rūpestingas ir atidus vartotojas turėjo visas galimybes pamatyti informaciją apie veiksmą, kurį tvirtina, ir susilaikyti nuo tolimesnių veiksmų. Vis dėlto ginčo byloje surinkti duomenys leidžia daryti išvadą, kad pareiškėjas, prieš suveddamas „Smart-ID“ programėlės PIN2 kodą, nekreipė deramo dėmesio į banko jam rodomą informaciją, suvedė „Smart-ID“ programėlės PIN2 kodą ir taip patvirtino ginčijamos mokėjimo operacijos įvykdymą.

Pareiškėjas, nors ir turėjo galimybę kritiškai įvertinti savo veiksmų su mokėjimo priemone riziką ir galimas pasekmes, nuo tolesnių veiksmų nesusilaikė, priešingai, vykdė visus trečiųjų asmenų nurodymus, net nepaisydamas to, kad bankas jam rodė tiek ginčijamos mokėjimo operacijos sumą, tiek ir lėšų gavėjo duomenis.

Kaip minėta, Taisyklių 11 punkte aiškiai reglamentuota, kad banko klientui suteiktų personalizuotų duomenų naudojimas yra skirtas duoti sutikimą įvykdyti mokėjimo operaciją. Ginčo byloje nėra duomenų, kad pareiškėjas būtų buvęs nesupažindintas su Taisyklėmis ar kad būtų jų nesupratęs.

Įvertinus pirmiau nurodytas aplinkybes, Lietuvos banko nuomone, galima daryti išvadą, kad pareiškėjas būtų galėjęs išvengti neautorizuotos mokėjimo operacijos iš savo sąskaitos įvykdymo, jeigu būtų buvęs pakankamai atidus ir kritiškas savo su mokėjimo priemone atliekamų veiksmų atžvilgiu ir būtų susilaikęs nuo veiksmų su savo mokėjimo priemone. Pareiškėjas galėjo suprasti, kad jo prašoma atlikti veiksmus, kuriais tvirtinamas mokėjimo operacijos įvykdymas, o bankas prieš ginčijamos mokėjimo operacijos įvykdymo patvirtinimą rodė tiek mokėjimo operacijos sumą, tiek lėšų gavėjo duomenis. Vis dėlto pareiškėjas į šią banko prieš mokėjimo operacijos įvykdymą rodytą informaciją nekreipė deramo dėmesio ir vykdė trečiųjų asmenų jam pateiktus nurodymus, tai ir lėmė, kad iš pareiškėjo banko sąskaitos buvo įvykdyta ginčijama mokėjimo operacija.

Lietuvos banko vertinimu, toks pareiškėjo elgesys gali būti pripažintas kaip elgesys, iš esmės besiskiriantis nuo atsargaus elgesio reikalavimų, tai galiausiai ir lėmė, kad pareiškėjas prarado savo mokėjimo priemonę, o tretieji asmenys įgijo galimybę jo vardu inicijuoti mokėjimo operaciją, kurią pareiškėjas pats patvirtino suveddamas „Smart-ID“ PIN2 kodą.

Taigi, įvertinus ginčo byloje turimus duomenis ir ginčo šalių paaiškinimus apie mokėjimo operacijų įvykdymo aplinkybes, galima teigti, kad pareiškėjas mokėjimo priemone naudojosi nesilaikydamas mokėjimo priemonės išdavimą ir naudojimą reglamentuojančių sąlygų ir neįvykdė Mokėjimų įstatymo 34 straipsnyje reglamentuojamų mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigų.

Visų ginčo byloje nustatytų aplinkybių kontekste galima daryti išvadą, kad pareiškėjo veiksmai, dėl kurių ji prarado mokėjimo priemonę, pasireiškė dideliu neatsargumu, tai galiausiai ir lėmė, jog buvo įvykdyta neautorizuota ginčijama mokėjimo operacija iš pareiškėjo sąskaitos ir pareiškėjas patyrė nuostolių.

Mokėjimų įstatymo 39 straipsnio 3 dalyje nustatyta, kad mokėtojai 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.

Be to, bankas, gavęs pareiškėjo pretenziją dėl neautorizuotos mokėjimo operacijos įvykdymo, nedelsdamas kreipėsi į lėšų gavėją banką, tačiau lėšų sugrąžinti nepavyko.

Įvertinus pirmiau išdėstytą informaciją, konstatuotina, kad yra pagrindas pareiškėjui

taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, todėl pareiškėjo reikalavimas bankui grąžinti neautorizuotos ginčijamos mokėjimo operacijos lėšų sumą yra nepagrįstas ir atmestinas.

2. Dėl lėšų pareiškėjo banko sąskaitoje saugumo.

Kaip minėta, nagrinėdamas ginčus Lietuvos bankas neatlieka patikrinimų tam, kad nustatytų, ar nebuvo pažeisti finansų įstaigų veiklai keliami teisės aktų reikalavimai. Lietuvos bankas remiasi ginčo šalių pateiktais konkrečiais įrodymais, kurių pagrindu priima sprendimą.

Vien tik pareiškėjo teiginiai, kad, įvykdydamas ginčijamą mokėjimo operaciją, bankas neužtikrino lėšų pareiškėjo banko sąskaitoje saugumo, savaime nepagrindžia fakto, kad banko taikytos klientų lėšų apsaugos priemonės buvo nepakankamos ir (ar) neatitinkančios teisės aktų reikalavimų ir būtent tai galėjo nulemti, kad pareiškėjas dėl mokėjimo operacijos įvykdymo patyrė nuostolių.

Duomenų, kad bankas būtų nevykdęs ar netinkamai vykdęs finansų rinką reglamentuojančių teisės aktų reikalavimus ir (ar) nesiėmęs priemonių užtikrinti savo klientų, įskaitant pareiškėjo, banke laikomų lėšų saugumo, nagrinėjant ginčą nenustatyta.

Į esminius šalių išdėstytus argumentus atsakyta, o kiti šalių nurodyti argumentai neturi esminės reikšmės sprendimo teisėtumui ir pagrįstumui, todėl dėl jų Lietuvos bankas plačiau nepasisako. Lietuvos banko pareiga priimti motyvuotą sprendimą neturėtų būti suprantama kaip reikalavimas detaliai atsakyti į kiekvieną šalių argumentą⁸.

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

Atmesti pareiškėjo X.X. reikalavimą.

Lietuvos banko sprendimas dėl ginčo esmės yra rekomendacinio pobūdžio ir teismui neskundžiamas. Vartotojui ir finansų rinkos dalyviui išlieka teisė dėl 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

⁸ Lietuvos Aukščiausiojo Teismo 2010 m. spalio 5 d. nutartis, priimta civilinėje byloje Nr. 3K-3-382/2010; 2010 m. gruodžio 20 d. nutartis civilinėje byloje Nr. 3K-3-536/2010 ir kt.