LIETUVOS BANKO PRIEŽIŪROS TARNYBOS FINANSINIŲ PASLAUGŲ IR RINKŲ PRIEŽIŪROS DEPARTAMENTO DIREKTORIUS

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

2020 m. balandžio 6 d. Nr. V 2020/(21.27.E-2101)-242-197
Vilnius

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

N u s t a t y t a:

Pareiškėjas su banku sudarė Interneto banko sutartį (toliau – sutartis), kurios sudėtinė dalis yra AB SEB banko bendrosios taisyklės (toliau – Taisyklės) ir Paslaugų interneto banke teikimo sąlygų aprašas (toliau – Aprašas). Šios sutarties pagrindu pareiškėjui buvo suteikta teisė elektroniniais kanalais atlikti banko operacijas, gauti informaciją, teikti pranešimus ir sudaryti sutartis, taip pat būti atpažįstamam (identifikuotam) nuotoliniu būdu banko, kitų SEB grupės įmonių ir trečiųjų asmenų interneto svetainių elektroninėse sistemose.

2020 m. vasario 10 d. pareiškėjas pastebėjo, kad, prisijungdamas prie interneto banko, be vartotojo identifikavimo kodo privalo papildomai įvesti ir asmens kodą. Nesutikdamas su tokios informacijos teikimu, pareiškėjas kreipėsi į banką ir prašė nurodyti, kokiu pagrindu bankas reikalauja tokių duomenų.

Įvertinęs pareiškėjo prašymą, 2020 m. vasario 12 d. bankas pareiškėjui pateikė atsakymą, kuriame pažymėjo, kad nuo 2020 m. sausio 28 d. įdiegė papildomą saugiklį klientams, kurie jungiasi prie interneto banko. Bankas taip pat nurodė, kad, jungiantis prie interneto banko iš naršyklės (ar kito įrenginio), iš kurios iki tol nebuvo prisijungta, interneto banko prisijungimo lange reikės papildomai įvesti asmens kodą. Pareiškėjas su tokiu banko pateiktu atsakymu nesutiko, todėl tarp šalių kilo ginčas.

Kreipimesi į Lietuvos banką dėl vartojimo ginčo nagrinėjimo pareiškėjas prašo įvertinti, ar pagrįstai bankas, jungiantis prie interneto banko, be pareiškėjo identifikavimo kodo, prašo papildomai įvesti asmens kodą. Pareiškėjas nurodo, kad bankas jam nepateikia informacijos, kokiu pagrindu reikalauja papildomų asmens duomenų. Pareiškėjo nuomone, asmens kodo pateikimas internete nėra saugus, todėl jis nesiruošia teikti tokių duomenų bankui. Pareiškėjo teigimu, bankas jam nepateikė išsamaus, motyvuoto, dokumentais pagrįsto atsakymo raštu, kodėl prisijungiant prie interneto banko yra prašoma papildomų duomenų, kurių nėra numatyta tarp šalių pasirašytoje sutartyje.

Bankas su pareiškėjo reikalavimu nesutiko ir prašė jį atmesti. Bankas nurodė, kad saugus el. bankininkystės naudojimas yra vienas svarbiausių banko prioritetų, todėl bankas nuolat tobulina saugumo priemones, jų naudojimo būdus bei procesus. Bankas paaiškino, kad, įvertinęs įvairias sukčiavimo schemas ir jų pasikartojimą, įdiegė papildomą saugiklį klientams, kurie prie interneto banko jungiasi naudodamiesi „Smart-ID" programėle ir mobiliuoju parašu, t. y. klientas, kiekvieną kartą jungdamasis prie interneto banko, prisijungimo lange turi papildomai suvesti asmens kodą. Banko nuomone, tai yra papildoma apsaugos priemonė, kurią bankas taiko, siekdamas sumažinti sukčiavimų atvejus, kai klientas, suklaidintas sukčių, tapęs socialinės inžinerijos auka, suveda prisijungimo priemonės PIN1 kodą ir atskleidžia sukčiams prieigą prie savo interneto banko paskyros. Bankas atkreipia dėmesį į tai, kad savo asmens kodą pareiškėjui reikia įvesti toje pačioje banko sistemos platformoje (aplinkoje), kurioje pareiškėjas veda ir kitus duomenis, todėl tvirtina, kad banko sistemoje visi klientų duomenys yra saugūs.

Bankas taip pat papildomai pažymėjo ir tai, kad, teikdamas paslaugas internetu, privalo atpažinti mokėjimo paslaugų vartotoją, t. y. tikrinti asmens, kuris jungiasi nuotoliniais

kanalais, tapatybę. Banko teigimu, mokėjimo paslaugų vartotojo tapatybei nuotoliniu būdu patvirtinti, taikomos autentiškumo patvirtinimo procedūras. Tokias procedūras bankas nustato savarankiškai, atsižvelgęs į mokėjimo paslaugų vartotojo naudojamas prisijungimo prie banko paslaugų internete priemones ir jų rūšį. Bankas nurodo, kad nors teisės aktai nenustato konkrečių rizikos valdymo būdų ir priemonių, tačiau nustato principus, kurių turi laikytis mokėjimo paslaugų teikėjai. Dėl šios priežasties bankas, įvertinęs paplitusius sukčiavimo scenarijus, kaip sukčiavimo rizikos mažinimo priemonę, pasirinko iš klientų, kurie nuotoliniu būdu jungiasi prie interneto banko, reikalauti įvesti asmens kodą. Asmens kodas yra unikalus skaičių derinys, žinomas mokėjimo paslaugų vartotojui, įprastai nežinomas sukčiams ir sunkiai atspėjamas. Banko nuomone, asmens kodas papildo vieną iš saugesnio kliento autentiškumo patvirtinimo elementų – „žinojimo elementą" (prisijungimo kodas, kurį sukčiai gali atspėti), ir padaro jį sudėtingesnį, t. y., norint prisijungti prie interneto banko paskyros, reikia žinoti ne tik prisijungimo kodą, tačiau ir asmens kodą. Atsižvelgdamas į tai, bankas mano pagrįstai reikalaujantis, kad pareiškėjas įvestų ne tik identifikavimo ir PIN1 kodą, tačiau papildomai įvestų asmens kodą, todėl prašo pareiškėjo reikalavimą atmesti 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 45 punktu, vartojimo ginčai Lietuvos banke nagrinėjami laikantis rungimosi, ginčų nagrinėjimo operatyvumo, koncentracijos, ekonomiškumo ir bendradarbiavimo principų. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Kaip matyti iš Lietuvos bankui pateiktų dokumentų ir informacijos, iš esmės tarp šalių ginčas kilo dėl jungiantis prie interneto banko papildomai prašomo įvesti asmens kodo pagrįstumo.

Mokėjimo paslaugų teikėjų veiklą, mokėjimo paslaugų teikimą, 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 (toliau – Mokėjimų įstatymas). Pagal Mokėjimų įstatymo 2 straipsnio 2 dalį, autentiškumo patvirtinimas yra procedūra, kuria mokėjimo paslaugų teikėjas *tikrina mokėjimo paslaugų vartotojo tapatybę* arba mokėjimo priemonės, įskaitant jos personalizuotus saugumo duomenis, naudojimo teisėtumą. Mokėjimo įstatymo 58 straipsnyje yra nustatyti autentiškumo patvirtinimo reikalavimai. Šio straipsnio 1 dalyje yra reglamentuota, kad mokėjimo paslaugų teikėjas privalo taikyti saugesnio autentiškumo patvirtinimo procedūrą, kai mokėtojas: 1) *internetu arba kitomis nuotolinio ryšio priemonėmis prisijungia prie savo mokėjimo sąskaitos*; 2) inicijuoja elektroninę mokėjimo operaciją; 3) nuotolinio ryšio priemone vykdo bet kokį veiksmą, kuris gali būti susijęs su sukčiavimo atliekant mokėjimą ar kitokio piktnaudžiavimo rizika. Mokėjimo įstatymo 2 straipsnio 56 dalyje taip pat yra nustatyta, kad saugesnis autentiškumo patvirtinimas yra autentiškumo patvirtinimas, kai saugiai naudojami bent du į žinojimo (tai, ką žino tik mokėjimo paslaugų vartotojas), turėjimo (tai, ką turi tik mokėjimo paslaugų vartotojas) ir būdingumo (tai, kas būdinga tik mokėjimo paslaugų vartotojui) kategorijas skirstomi elementai, o pažeidus vieną elementą neturi sumažėti kitų elementų patikimumas.

Vadovaudamiesi 2017 m. lapkričio 27 d. Europos komisijos deleguotojo reglamento (ES) 2018/389, kuriuo Europos Parlamento ir Tarybos direktyva (ES) 2015/2366 papildoma griežto kliento autentiškumo patvirtinimo ir bendrų ir saugių atvirųjų ryšių standartų techniniais reguliavimo standartais (toliau – Reglamentas), 28 straipsnio 1 dalimi, mokėjimo paslaugų teikėjai, įskaitant banką, turi užtikrinti saugų identifikavimą atliekant elektroninius mokėjimus, kai užmezgamas ryšys tarp mokėtojo prietaiso ir gavėjo priėmimo prietaiso, įskaitant, be kita ko, mokėjimo terminalus. Šio straipsnio 2 dalyje yra nustatyta pareiga užtikrinti, kad veiksmingai būtų sumažinta rizika, kad perduodami duomenys bus perduoti neturinčioms leidimo šalims naudojant mobiliąsias programas ir kitas mokėjimo paslaugų vartotojų sąsajas, kuriomis teikiamos elektroninių mokėjimų paslaugos.

Aprašo 6 punkte yra nustatyta, kad bankas, norėdamas užtikrinti saugias kliento operacijas ir patikrinti autentiškumą, suteikia naudotojui personalizuotus saugumo duomenis – apsaugos ir atpažinimo priemones, taip pat gali sutikti, kad naudotojas naudotų savo pasirinktas atpažinimo priemones: 1) atpažinimo priemonės: atpažinimo kodas, laikinas slaptažodis, PIN kodas, mobiliųjų įrenginių biometrinės apsaugos priemonės; 2) banko išduotos atpažinimo priemonės: slaptažodžių kortelė ir slaptažodžių generatorius.

Taisyklių 15 skyriuje yra įtvirtinta, kad autentiškumo patvirtinimas yra procedūra, kurią bankas atlieka *tikrindamas banko klientų tapatybę*, mokėjimo priemonės, įskaitant jos personalizuotus saugumo duomenis, naudojimo teisėtumą. Taisyklių 13 skyriuje yra nustatyta, kad *bankas naudojasi banko klientų asmens duomenimis ir kita informacija, konsultuodamas pareiškėją ar teikdamas jam jo pageidaujamas banko paslaugas*, taip pat informuodamas pareiškėją apie naujas ar patobulintas paslaugas. Ši informacija yra būtina nustatant banko klientų asmens tapatybę ir užtikrinant pareiškėjų lėšų bei informacijos saugumą. Informaciją apie pareiškėjo duomenų tvarkymą bankas pateikia SEB įmonių Lietuvoje asmens duomenų tvarkymo politikoje. Pagal SEB įmonių Lietuvoje asmens duomenų tvarkymo politiką, bankas turi teisę rinkti pagrindinius asmens duomenis, tokius kaip vardas, pavardė, asmens kodas, gimimo data, ir identifikavimo duomenis, tokius kaip asmens dokumentų duomenys, IP adresas, interneto banko prisijungimo duomenys bei kita naršymo informacija, įskaitant duomenis apie tai, kada ir iš kur buvo prisijungta prie interneto banko ir interneto svetainės ar kitų elektroninių platformų.

Vertinant abiejų šalių pateiktus duomenis, svarbu pažymėti, kad pareiškėjas nurodo, kad bankas nepagrįstai, pareiškėjui jungiantis prie interneto banko, papildomai prašo pateikti asmens kodą. Nesutikdamas su tokiais pareiškėjo kreipimesi išdėstytais argumentais, bankas nurodo, kad, įvertinęs paplitusius sukčiavimo scenarijus, kaip sukčiavimo rizikos mažinimo priemonę pasirinko iš klientų, kurie nuotoliniu būdu jungiasi prie interneto banko, reikalauti įvesti asmens kodą. Banko teigimu, asmens kodas yra unikalus skaičių derinys, žinomas mokėjimo paslaugų vartotojui, įprastai nežinomas sukčiams ir sunkiai atspėjamas. Dėl šios priežasties bankas mano pagrįstai, siekdamas užtikrinti autentiškumo patvirtinimą, prisijungiant prie interneto banko, reikalauja, kad pareiškėjas papildomai pateiktų asmens kodą.

Lietuvos banko vertinimu, teisės aktų leidėjas nėra reglamentavęs konkrečių priemonių, kuriomis mokėjimo paslaugų teikėjas gali tinkamai atlikti autentiškumo patvirtinimą. Taigi, šiuo atveju mokėjimo paslaugų teikėjams palikta teisė patiems nustatyti rizikos valdymo ir jos mažinimo būdus, taip pat pasirinkti konkrečias autentiškumo priemones. Iš Lietuvos bankui pateiktų duomenų matyti, kad šalys, sudarydamos sutartį, susitarė taikyti konkrečias atpažinimo ir apsaugos priemones (Aprašo 6 punktas). Tačiau svarbu pažymėti, kad, be šių atpažinimo ir apsaugos priemonių, šalys taip pat susitarė, kad bankas turi teisę naudotis pareiškėjo asmens duomenimis ir kita informacija, konsultuodamas pareiškėją *ar teikdamas jam jo pageidaujamas banko paslaugas*, taip pat informuodamas pareiškėją apie naujas ar patobulintas paslaugas (Taisyklių 13 skyrius). Atsižvelgiant į teisės aktų reikalavimus, kuriuose bankui yra numatyta pareiga taikyti saugesnio autentiškumo patvirtinimo procedūrą, kai mokėtojas internetu arba kitomis nuotolinio ryšio priemonėmis prisijungia prie savo mokėjimo sąskaitos, taip pat į tarp šalių sudarytos sutarties nuostatas, kuriose yra įtvirtinta, kad bankas naudojasi pareiškėjo asmens duomenimis, kai pareiškėjui teikia jo pageidaujamas banko paslaugas, galima daryti išvadą, kad bankas, siekdamas kiek įmanoma sumažinti sukčiavimo riziką, pagrįstai, be Apraše numatytų atpažinimo ir apsaugos priemonių, prisijungiant prie interneto banko papildomai reikalauja ir pareiškėjo asmens kodo tam, kad būtų tinkamai atliktas pareiškėjo autentifikavimas ir kad būtų sumažinta sukčiavimo rizika.

Teisės aktai įpareigoja mokėjimo paslaugų teikėjus nuolat vertinti, ar veiklos aplinkos pokyčiai daro įtaką esamoms saugumo priemonėms ir ar reikia įdiegti papildomų rizikos mažinimo priemonių, keisti galiojančias saugumo priemones, naudojamas technologijas ir procedūras ar siūlomas mokėjimo paslaugas, siekiant kuo labiau sumažinti galimus operacinius arba saugumo incidentus, sukčiavimą ir galimą neigiamą poveikį teikiant mokėjimo paslaugas (Lietuvos banko 2018 m. gruodžio 20 d. nutarimu Nr. 03-264 patvirtinto Operacinės ir saugumo rizikos valdymo reikalavimų mokėjimo paslaugų teikėjams aprašo 22 punktas).

Vadovaujantis Mokėjimų įstatymo 35 straipsnio 1 dalies 1 punktu, mokėjimo paslaugų teikėjai, įskaitant banką, turi užtikrinti, kad, be mokėjimo priemonės vartotojo, turinčio teisę naudotis mokėjimo priemone, personalizuotais saugumo duomenimis negalėtų naudotis kiti asmenys. Mokėjimo įstatymas nenumato konkrečių priemonių, kuriomis mokėjimo paslaugų teikėjai turi užtikrinti prieš tai nurodyto reikalavimo vykdymą. Atsižvelgdamas į tai, kad interneto erdvėje nuolat daugėja sukčiavimo atvejų, kai tretieji asmenys neteisėtai bando išvilioti iš asmenų jų prisijungimo prie internetinės bankininkystės sistemos duomenis, siekdami įgyti galimybę neteisėtai pasinaudoti banko sąskaitose esančiomis lėšomis, bei į tai, kad nustatyti tokius neteisėtus veiksmus atlikusius asmenis dėl jų taikomų sudėtingų

sukčiavimo schemų yra itin sudėtinga, o mokėjimo priemonių turėtojai ne visada sugeba laiku suprasti, kad atskleidžia prisijungimo prie jiems išduotų mokėjimo priemonių duomenis tokių duomenų neturintiems teisės gauti tretiesiems asmenims, Lietuvos bankas mano, kad mokėjimo paslaugų teikėjai, įskaitant banką, gali ir turi imtis visų teisėtų saugumo priemonių, įskaitant tas, kuriomis mokėjimo paslaugų teikėjo suteikti saugumo duomenys būtų kombinuojami su kita, tik mokėjimo priemonės turėtojui žinoma informacija, net ir tais atvejais, kai tokios saugumo priemonės nebuvo iš anksto konkrečiai aptartos tarp mokėjimo priemonėms turėtojo ir mokėjimo paslaugų teikėjo sudarytose sutartyse.

Pažymėtina, kad nagrinėjant ginčą faktinių aplinkybių, kurios leistų pagrįstai manyti, kad asmens kodui suvesti toje pačioje banko sistemos platformoje, kurioje prašoma suvesti ir kitus pareiškėjui atpažinti būtinus duomenis (pvz., PIN1 kodą), bankas taikytų kitokias nei kitiems duomenims taikomas saugumo priemones, nenustatyta. Aplinkybių, kurios leistų įtarti, kad banko prašymas suvesti asmens kodą, pareiškėjui jungiantis prie savo internetinės bankininkystės sistemos paskyros, būtų susijęs su kitais nei paties pareiškėjo tinkamo atpažinimo, jam išduotų mokėjimo priemonių naudojimo teisėtumo patikrinimo bei tokių priemonių ir jų saugumo kodų saugumo užtikrinimo tikslais, taip pat nenustatyta.

Lietuvos banko nuomone, banko prašymas jungiantis prie internetinės bankininkystės sistemos paskyros papildomai suvesti asmens kodą nelaikytinas esminiu tarp pareiškėjo ir banko sudarytos sutarties dėl mokėjimo paslaugų teikimo pakeitimu ir (arba) aplinkybe, kuri iš esmės pakeistų sutartinių prievolių pusiausvyrą, dėl kurios vykdyti sutartį vienai iš sutarties šalių taptų sudėtingiau negu kitai šaliai, kaip tai reglamentuota Lietuvos Respublikos civilinio kodekso (toliau – CK) 6.204 straipsnyje. Lietuvos banko vertinimu, minėtas prašymas neprieštarauja nei teisės aktų, nei tarp šalių sudarytos sutarties nuostatoms, nepanaikina ir (arba) iš esmės nepakeičia sutartimi pareiškėjui ir bankui suteikiamų teisių ir pareigų, sutarties šalių atsakomybės apimties bei banko teiktų pareiškėjui paslaugų pobūdžio ar turinio, taip pat neprieštarauja protingumo, sąžiningumo ir teisingumo kriterijams (CK 6.186 straipsnis), todėl darytina išvada, kad nėra pagrindo tokio banko prašymo laikyti neteisėtu.

Atsižvelgiant į visa tai, kas išdėstyta pirmiau, darytina išvada, kad nagrinėjamu atveju bankas tinkamai vykdo sutartyje ir teisės aktuose įtvirtintas pareigas, imasi papildomų priemonių tam, kad būtų atliktas pareiškėjo autentiškumo patvirtinimas ir kad būtų išvengta sukčiavimo rizikos, todėl pagrįstai, be Aprašo 6 punkte nurodytų atpažinimo ir apsaugos priemonių, jungiantis prie interneto banko papildomai prašo suvesti asmens kodą, kuris atitinka teisės aktuose numatyto saugesnio autentiškumo patvirtinimo požymius. Dėl šios priežasties pareiškėjo argumentas, kad bankas nepagrįstai jungiantis prie interneto banko prašo papildomai pateikti asmens kodą, yra atmestinas kaip nepagrįstas.

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 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.

Reguliuojamos rinkos priežiūros skyriaus
viršininkas, pavaduojantis Finansinių paslaugų
ir rinkų priežiūros departamento direktorių Vaidas Cibas