



**LIETUVOS BANKO  
FINANSŲ RINKOS PRIEŽIŪROS TARNYBOS  
TEISĖS IR LICENCIJAVIMO DEPARTAMENTO  
DIREKTORIUS**

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

2021 m. spalio 28 d. Nr. 429-385  
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. gegužės 14 d. nuo 13 val. 11 min. iki 13 val. 41 min. (Lietuvos laiku), panaudojant pareiškėjos vardu banko išduotos mokėjimo kortelės „Debit MasterCard bekontaktė“ Nr. (*duomenys neskelbtini*) (toliau – kortelė) duomenis, buvo inicijuotos aštuonios mokėjimo operacijos, kurių bendra suma – 11 285 Eur, lėšas pervedant lėšų pervedimų tarpininkui *TransferGo Ltd.* (toliau – *TransferGo*)<sup>1</sup>.

2021 m. gegužės 14 d. 14 val. 50 min. pareiškėja kreipėsi telefonu į banką prašydama patikrinti jos sąskaitą. Pareiškėja informavo, kad jai skambino rusakalbiai asmenys, kurie nurodė, kad „mato vagystės iš pareiškėjos sąskaitos mėginimą“, ir tam, kad galėtų sustabdyti lėšų nurašymą, paprašė pareiškėjos pateikti priegios prie su kortele susietos sąskaitos duomenis. Pokalbio metu pareiškėja pripažino atskleidusi skambinusiems asmenims savo duomenis (interneto banko atpažinimo kodą). Pareiškėja taip pat informavo, kad gavo informacinę žinutę dėl užpildytos kredito paraiškos, nors ji jos neteikė, ir paprašė šią paraišką atšaukti. Pokalbio metu banko darbuotoja užblokavo pareiškėjos kortelę ir interneto banko paskyrą, vėliau atšaukė pareiškėjos vardu pateiktą vartojimo kredito paraišką 3 000 Eur (15 val. 36 min.). To paties telefoninio pokalbio metu banko darbuotoja patikrino pareiškėjos vardu sudarytas „Smart-ID“ tapatybės patvirtinimo priemonės sutartis ir informavo pareiškėją, kad 2021 m. gegužės 14 d. pareiškėjos vardu buvo sukurta nauja prisijungimo priemonė – programėlė „Smart-ID“ kitame telefono įrenginyje, todėl patarė pareiškėjai nedelsiant kreiptis į „Smart-ID“ tapatybės patvirtinimo priemonę sukūrusią ir prižiūrinčią įmonę „SK ID Solutions AS“ dėl „Smart-ID“ paskyros blokavimo ir panaikinimo, o dėl galimo sukčiavimo, duomenų atskleidimo kitiems asmenims – į policiją.

2021 m. gegužės 14 d. (15 val. 40 min.) banko darbuotoja perskambino pareiškėjai ir, nepastebėjusi pareiškėjos su kortele susietoje sąskaitoje lėšų, rezervuotų mokėjimo operacijoms, kurios buvo inicijuotos panaudojant kortelės duomenis nuo 13 val. 11 min. iki 13 val. 41 min., įvykdyti, informavo pareiškėją, kad jos mokėjimo sąskaitoje paskutinė atlikta mokėjimo operacija yra lėšų pervedimas UAB „Tele2“, taip pat nurodė, kad pareiškėjos sąskaita, susieta su kortele, tiek ir pati kortelė yra užblokuotos, todėl pareiškėjos lėšos yra saugios. Pareiškėja telefoninio pokalbio su banko darbuotoja metu patvirtino, kad atskleidė tretiesiems asmenims elektroninės bankininkystės informaciją – padiktavo interneto banko atpažinimo kodą.

2021 m. gegužės 17 d. pareiškėja telefonu banko darbuotojo buvo informuota, kad 2021 m. gegužės 14 d. buvo įvykdytos aštuonios mokėjimo operacijos, panaudojant kortelės duomenis, ir lėšos už šias mokėjimo operacijas bus nurašytos iš pareiškėjos su kortele susietos sąskaitos. Tą pačią dieną pareiškėja pateikė pretenziją bankui dėl nurašytų lėšų už 2021 m. gegužės 14 d. mokėjimo operacijas grąžinimo.

<sup>1</sup> *TransferGo* vykdo savo veiklą Jungtinėje Karalystėje ir yra prižiūrima šios šalies priežiūros institucijų. Kaip nurodo bankas atsiliėpime Lietuvos bankui, pareiškėjos banko sąskaitos išrašė mokėjimo operacijų laikas atvaizduojamas pagal tai, kada mokėjimo operacijos įvyko *TransferGo* buveinės vietos (Jungtinės Karalystės) laiku, todėl išrašė nurodytas laikas nuo 11 val. 11 min. iki 11 val. 41 min., t. y. reikia pridėti 2 valandas, kad gautume Lietuvos laiko juostą.

2021 m. birželio 22 d. bankas, atsakydamas į pareiškėjos pretenziją, nurodė, kad neturi teisinio pagrindo gražinti lėšų už pareiškėjos ginčijamas 2021 m. gegužės 14 d. mokėjimo operacijas.

Nesutikdama su banko atsakymu, pareiškėja kreipėsi į Lietuvos banką dėl ginčo nagrinėjimo. Pareiškėja ginčija banko veiksmus, negražinant ginčijamų mokėjimo operacijų sumų. Kreipimesi Lietuvos bankui pareiškėja teigia, kad 2021 m. gegužės 14 d. ji tapo sukčių auka ir prarado 10 100 Eur. Pareiškėja nurodo, kad jai kelia abejonių banko taikomos saugumo procedūros, pareiškėjos prašymo gražinti ginčijamų mokėjimo operacijų lėšas įvykdymo tinkamumas, taip pat nesuprantamos priežastys, dėl kurių bankas atsisakė pareiškėjai pateikti jos ir banko darbuotojų pokalbių įrašus. Kreipimesi pažymima, kad šiuo metu tęsiasi policijos tyrimas dėl vagystės, tačiau, pareiškėjos teigimu, ji žino, kad atgauti pinigus, pervestus į užsienio sąskaitą ar sąskaitas, bus beveik neįmanoma, todėl vienintelė galimybė pinigus apsaugoti buvo bankui užblokuoti visas prieigas ir visus pervedimus arba prašyti užblokuoti išėjusius pervedimus tarpininko įmonėje, tačiau bankas to tinkamai nepadarė, taip pat neinformavo pareiškėjos apie galimybę kreiptis į tarpininko įmonę dėl ginčijamų mokėjimo operacijų atšaukimo. Pareiškėja pažymi, kad tik policijos pareigūno patarta kreipėsi į tarpininko įmonę (*TransferGo*), į kurią buvo pervesti pinigai prieš pasiekiant tikslinę sąskaitą, ir, paaiškinus visą situaciją, pavyko atšaukti paskutinį (aštuntąjį) mokėjimą ir susigražinti 1 185 Eur. Pareiškėjos vertinimu, banko neveikimas ir (ar) netinkamas veikimas, vykdant pareiškėjos prašymą atšaukti ginčijamas mokėjimo operacijas, lėmė tai, kad ginčijamų mokėjimo operacijų lėšos buvo pervestos sukčiams, todėl kreipimusi pareiškėja prašo rekomenduoti bankui gražinti 10 100 Eur.

Bankas nesutinka tenkinti pareiškėjos reikalavimo. Atsiliepime pažymima, kad pareiškėja ir bankas, sudarydami Interneto banko sutartį ir Kortelės sutartį, susitarė dėl sutikimo įvykdyti mokėjimo operacijas, panaudojant kortelę, davimo formos ir tvarkos. Atsiliepime nurodoma, kad banko vidaus sistemose buvo užfiksuoti duomenys, liudijantys, kad pareiškėjos ginčijamos mokėjimo operacijos buvo inicijuotos suvedant kortelės duomenis ir tik pareiškėjai žinomus prisijungimo prie interneto banko duomenis. Taigi, bankas mano, kad pareiškėjos ginčijamos mokėjimo operacijos turi būti laikomos jos autorizuotomis, nes joms buvo duotas sutikimas banko ir pareiškėjos sutarta forma bei tvarka. Be to, bankas atkreipia dėmesį, kad buvo nustatytos ir sąlygos vertinti pareiškėjos elgesį kaip itin neatsargų: pareiškėja atskleidė personalizuotus saugumo elementus tretiesiems asmenims, taigi, nesilaikė elementarių saugumo reikalavimų. Dėl šios priežasties bankas mano, kad pareiškėja yra visiškai atsakinga dėl nuostolių, kurių turėjo atlikus ginčijamas mokėjimo operacijas trečiųjų asmenų naudai. Atsiliepime, be kita ko, pažymėta, kad pareiškėjos ginčijamos mokėjimo operacijos buvo atliktos ir patvirtintos, taikant saugesnę autentiškumo nustatymo procedūrą, 2021 m. gegužės 14 d. nuo 13 val. 11 min. iki 13 val. 41 min. Lietuvos laiku – taigi, dar iki telefoninio pokalbio su banko darbuotoja ir iki kortelės užblokavimo (iki 14 val. 50 min. Lietuvos laiku), o lėšos iš pareiškėjos sąskaitos, susietos su kortele, nurašytos 2021 m. gegužės 17 d., kai banke, pagal „MasterCard“ organizacijos taisykles, buvo gautas *TransferGo* ginčijamų mokėjimo operacijų patvirtinimas. Bankas pažymi, kad, pagal „MasterCard“ organizacijos taisykles, mokėjimo operacijas galima ginčyti kaip atliktas neteisėtai, t. y. be pareiškėjos žinios (angl. *fraud*), tuo atveju, jei mokėjimo operacijos nėra autorizuotos (patvirtintos) „3D Secure“ kodu. Bankas nurodė, kad nagrinėjamu atveju, atsižvelgiant į tai, jog mokėjimo operacijos buvo patvirtintos „3D Secure“ kodu, vadovaujantis „MasterCard“ organizacijos taisyklėmis, ginčyti šių operacijų, kaip neteisėtų, t. y. atliktų be pareiškėjos žinios, bankas neturi galimybės, nes neturi ginčo teisės. Atsižvelgdamas į pareiškėjos kreipimesi nurodytus teiginius, bankas papildomai informuoja, kad neriboja pareiškėjos teisės susipažinti su telefoninių pokalbių tarp jos ir banko darbuotojos įrašais, ir gali suteikti pareiškėjai galimybę išklausti šiuos telefoninius pokalbius banko skyriuje. Banko teigimu, jis telefoninių pokalbių įrašų kopijų klientams neteikia, nes neturi galimybės užtikrinti įrašo konfidencialumo ar valdyti netinkamo panaudojimo rizikas. Atsiliepimu bankas prašo atmesti pareiškėjos 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 45 punktu, vartojimo ginčai Lietuvos banke nagrinėjami laikantis rungimosi, ginčų nagrinėjimo operatyvumo, koncentracijos, ekonomiškumo ir bendradarbiavimo principų. Nagrinėdamas ginčą Lietuvos bankas vertina pateiktus įrodymus ir to pagrindu priima sprendimą.

Pareiškėjos ir banko ginčas kilo dėl banko atsisakymo grąžinti pareiškėjai jos vardu banke atidarytoje sąskaitoje septynių iš aštuonių 2021 m. gegužės 14 d., panaudojus kortelės duomenis, atliktų mokėjimo operacijų lėšas iš viso – 10 100 Eur<sup>2</sup> (toliau – ginčijamos mokėjimo operacijos). Pareiškėja teigia, kad ji neautorizavo ginčijamų mokėjimo operacijų, informavo banką apie tai, kad ji galėjo tapti sukčių auka, ir paprašė banko atšaukti šias operacijas (joms, kaip ji teigia, nedavė sutikimo), kai bankas dar turėjo galimybę tai padaryti (t. y. nepervesti lėšų į gavėjų banko sąskaitą, nes lėšos pareiškėjos banko sąskaitoje buvo dar tik rezervuotos), todėl bankas turi grąžinti pareiškėjai ginčijamų mokėjimo operacijų sumas. Bankas teigia, kad pareiškėjos ginčijamos mokėjimo operacijos buvo tinkamai, t. y. šalių sutarta forma ir tvarka, autorizuotos, be to, yra sąlygos pareiškėjos elgesi, įvykdant ginčijamas mokėjimo operacijas, vertinti kaip labai neatsargų, todėl bankas mano, kad neturi pareigos kompensuoti pareiškėjai jos nuostolių dėl ginčijamų mokėjimo operacijų.

Siekiant išspręsti tarp pareiškėjos ir banko kilusį ginčą, Lietuvos banko vertinimu, būtina nustatyti šias pagrindines aplinkybes: 1) ar ginčijamos mokėjimo operacijos laikytinos autorizuotomis, t. y. ar šioms operacijoms atlikti buvo gautas pareiškėjos sutikimas; 2) ar bankas turėjo (turi) pareigą grąžinti pareiškėjai ginčijamų mokėjimo operacijų sumas.

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.

#### *Dėl ginčijamų mokėjimo operacijų autorizavimo*

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).

Mokėjimų įstatymo 37 straipsnio 1 dalyje nustatyta, kad tuo atveju, jeigu mokėtojas neigia autorizavęs įvykdytą mokėjimo operaciją ar teigia, kad mokėjimo operacija buvo įvykdyta netinkamai, jo mokėjimo paslaugų teikėjas turi įrodyti, kad mokėjimo operacijos autentiškumas buvo patvirtintas, ji buvo tinkamai užregistruota, įrašyta į sąskaitas ir jos nepaveikė techniniai trikdžiai arba kiti mokėjimo paslaugų teikėjo teikiamos paslaugos trūkumai; kai mokėtojas neigia autorizavęs įvykdytą mokėjimo operaciją, mokėtojo mokėjimo paslaugų teikėjo arba atitinkamais atvejais mokėjimo inicijavimo paslaugos teikėjo užregistruotas mokėjimo priemonės naudojimas nebūtinai yra pakankamas įrodymas, kad mokėtojas autorizavo mokėjimo operaciją ar veikė nesąžiningai arba tyčia ar dėl didelio neatsargumo neįvykdė vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų.

Pažymėtina, kad Mokėjimų įstatyme nėra nustatytų konkrečių mokėtojo sutikimo įvykdyti mokėjimo operaciją būdų ir (arba) išsamios tokio sutikimo davimo tvarkos. Vadovaujantis Mokėjimų įstatymo 13 straipsnio 3 dalies 3 punktu ir 29 straipsnio 1 punktu, mokėtojo sutikimo įvykdyti mokėjimo operaciją davimo sąlygos ir tvarka turi būti aptartos mokėtojo ir jo mokėjimo paslaugų teikėjo sudaromoje bendrojoje mokėjimo paslaugų teikimo sutartyje (toliau – bendroji sutartis).

Banko teigimu, pareiškėjos ginčijamos mokėjimo operacijos turi būti laikomos autorizuotomis, nes buvo atlikti veiksmai, reikalingi mokėjimo operacijoms kortele inicijuoti, t. y. sutikimas mokėjimo operacijoms suformuoti ir vykdyti buvo duotas vienu iš pareiškėjos ir banko sudarytoje bendrojoje sutartyje nurodytų būdų – panaudojant kortelės duomenis (kortelės numerį, galiojimo laiką, CVC kodą) ir suvedant interneto banko prisijungimo duomenis (interneto banko naudotojo ID kodą ir atpažinimo priemonės „Smart-ID“ PIN1 ir PIN2 kodus).

Kaip nurodo bankas atsiliepime, pareiškėja ir bankas, sudarydami Interneto banko sutartį bei Kortelės sutartį, susitarė dėl sutikimo įvykdyti mokėjimo operacijas, panaudojant kortelę, davimo formos ir tvarkos. Mokėjimo operacijos patvirtinimo būdas, panaudojant kortelę, aptartas banko Bendrųjų taisyklių (toliau – Taisyklės), kurios yra neatskiriama bet kurios banko ir jo kliento sudarytos sutarties dalis<sup>3</sup>, 2 priede („Mokėjimo kortelių išdavimo ir naudojimo taisyklės“). Priedo 11 skyriuje nustatyta, kad mokėtojas duoda sutikimą mokėti

<sup>2</sup> 2021 m. gegužės 14 d. atlikto aštuntojo mokėjimo lėšas į pareiškėjos sąskaitą grąžino lėšų pervedimo tarpininkas (*TransferGo*).

<sup>3</sup> Taisyklių 1 skyriaus nuostatos („Bendrosios taisyklės ir kainynas, kuriuos galite rasti tinklalapyje, taikomi teikiant visas mūsų paslaugas.“)

mokėjimo kortele, jei, atsiskaitydamas elektroninės prekybos ar paslaugų vietose, įveda mokėjimo kortelės duomenis: mokėjimo kortelės numerį, galiojimo laiką, CVC kodą; pateikia mokėjimo kortelės ir (ar) savo duomenis prekybininkui ar paslaugos teikėjui ir patvirtina mokėjimo operaciją „3D Secure“ būdu.

Atkreiptinas dėmesys į tai, kad Taisyklių 2 priedo 11 skyriuje aprašomi atvejai, kai mokėtojas duoda savo sutikimą pervesti lėšas mokėjimo kortele prekybininkui arba paslaugų teikėjui, su kuriuo mokėtojas nori atsiskaityti, ir tuo tikslu perduoda mokėjimo kortelės ir kitus šioje Taisyklių nuostatoje nurodytus duomenis, o nagrinėjamo ginčo atveju – priešingai, nei nurodyta minimoje Taisyklių nuostatoje, pareiškėja šiuos duomenis atskleidė ne dėl to, kad ketino kortele pervesti lėšas (atsiskaityti), o, kaip pati teigia, paprašyta trečiųjų asmenų, prisistačiusių banko darbuotojais, siekiant patikrinti įtartą veiklą jos su kortele susietoje sąskaitoje ir sustabdyti galimai neteisėtą bandymą nurašyti lėšas iš šios pareiškėjos banke atidarytos sąskaitos. Taigi, pareiškėja, tiek bendraudama su banku dėl ginčijamų mokėjimo operacijų, tiek ir kreipimesi į Lietuvos banką nuosekliai laikosi pozicijos, kad valios inicijuoti ir įvykdyti ginčijamų mokėjimo operacijų ji neišreiškė ir nedavė tam savo sutikimo (neautorizavo ginčijamų mokėjimo operacijų) šalių sutarta forma ir tvarka.

Pažymėtina, kad bankas, darydamas išvadą, jog ginčijamos mokėjimo operacijos buvo autorizuotos Taisyklėse nustatyta (šalių sutarta) tvarka, iš esmės remiasi tik tuo faktu, kad mokėjimo operacijai įvykdyti buvo panaudoti kortelės duomenys ir suvesti prisijungimo prie interneto banko prisijungimo duomenys, tačiau nevertina, kuriuo metu ir (arba) kas perdavė lėšų gavėjui ir (arba) jo mokėjimo paslaugų teikėjui duomenis, kurių pagrindu buvo inicijuotos ginčijamos mokėjimo operacijos, t. y. ar šiuos duomenis tiesiogiai pateikė pati pareiškėja, ar iš pareiškėjos šiuos duomenis neteisėtai išvilioję (mokėjimo priemonę neteisėtai pasisavinę) asmenys.

Bankas pateikė jo vidaus sistemose užfiksuotus duomenis, pagrindžiančius, kad ginčijamos mokėjimo operacijos buvo autorizuotos panaudojant „3D Secure“ kodą, t. y. taikant saugesnio autentiškumo patvirtinimo procedūrą. Tačiau vien šie duomenys, Lietuvos banko vertinimu, dar neįrodo, kad visi šie veiksmai atlikti pareiškėjos sutikimu, t. y. kad mokėjimo nurodymai atlikti kredito pervedimus (ginčijamas mokėjimo operacijas) iš tiesų atlikti pareiškėjos valia ir su jos sutikimu. Kaip minėta pirmiau, remiantis Mokėjimų įstatymo nuostatomis, vien aplinkybė, kad mokėtojo mokėjimo paslaugų teikėjo vidaus sistemose užregistruotas mokėtojui išduotos mokėjimo priemonės, įskaitant jos personalizuotus saugumo duomenis, naudojimas, nelaikytina pakankamu įrodymu, jog mokėjimo priemone naudojosi ir (arba) mokėjimo operaciją autorizavo pats mokėtojas (Mokėjimų įstatymo 37 straipsnio 3 dalis).

Bankas, siekdamas pagrįsti savo poziciją, t. y. kad ginčijamos mokėjimo operacijos buvo inicijuotos ir įvykdytos šalių sutarta forma ir tvarka – panaudojant tik pareiškėjai žinomus kortelės duomenis (kortelės numerį, galiojimo laiką, CVC kodą) ir suvedant interneto banko prisijungimo duomenis (interneto banko naudotojo ID kodą ir „Smart-ID“ paskyros PIN1 ir PIN2 kodus), pateikė banko informacinės sistemos žurnalo įrašus (pareiškėjos jungimosi įrašai prie interneto banko), iš kurių matyti, kad IP adresą (*duomenys neskelbtini*) pareiškėja naudojo pirmiau (iki 2021 m. gegužės 14 d.), ginčijamų operacijų metu ir po 2021 m. gegužės 14 d., jungdamasi prie savo interneto banko iš to paties įrenginio. Banko teigimu, „Smart-ID“ naujos paskyros, kurią sukčiai galėjo instaliuoti kitame (ne pareiškėjos) įrenginyje, sukūrimą pareiškėja patvirtino esamos „Smart-ID“ tapatybės patvirtinimo priemonės PIN1 ir PIN2 kodais ir tokiu būdu nauja „Smart-ID“ paskyra buvo sukurtas sukčių įrenginyje. Taigi, banko teigimu, pareiškėja, suvedusi „Smart-ID“ paskyros PIN1 ir „Smart-ID“ paskyros PIN2 kodus savo telefone, patvirtino „Smart-ID“ paskyros sukūrimą kitame įrenginyje (jis galėjo būti sukčių kontroliuojamas), kuriame sukčiai galėjo atlikti ir tolesnius veiksmus: 2021 m. gegužės 14 d. (13 val. 8 min.) padidintas mokėjimų, panaudojant kortelę, limitas (nuo 3 000 iki 20 000 Eur)<sup>4</sup>, nuo 13 val. 11 min. iki 13 val. 41 min. inicijuotos ir įvykdytos ginčijamos mokėjimo operacijos kortele, jas patvirtinus „3D Secure“ kodu, pareiškėjos vardu taip pat pateikta vartojimo kredito paraiška 3 000 Eur. Tokias banko nurodytas aplinkybes patvirtina ir pareiškėjos kreipimesi nurodyta aplinkybė: t. y. kreipimesi pareiškėja pripažįsta, kad tretiesiems asmenims atskleidė

<sup>4</sup> Pareiškėja kreipimesi teigia, kad jai nėra suprantamos aplinkybės, dėl kurių buvo įvykdytos ginčijamos mokėjimo operacijos, nes jos, pareiškėjos teigimu, viršijo pareiškėjai nustatytus dienos (1 158,48 Eur) ir mėnesio (4 344,30 Eur) operacijų limitus. Vis dėlto, kaip atsiliepiame atkreipė dėmesį bankas, interneto banke nustatyti mokėjimo operacijų limitai nėra taikomi mokėjimo operacijoms, inicijuotoms panaudojant mokėjimo korteles. Ginčijamų mokėjimo operacijų atlikimo dieną interneto banke nustatyti dienos ir mėnesio operacijų limitai nebuvo pakeisti.

prisijungimo prie interneto banko duomenis ir kartą per turimą „Smart-ID“ tapatybės patvirtinimo priemonę, paprašyta trečiųjų asmenų, suvedė „Smart-ID“ paskyros PIN2 kodą. Kita vertus, būtina pažymėti ir tai, kad ginčo byloje nėra duomenų (jų nepateikė ir bankas kartu su atsiliepimu), iš kurio galinio įrenginio (konkreto IP adreso) buvo patvirtintos pareiškėjos ginčijamos mokėjimo operacijos. Vis dėlto, kaip matyti iš atsiliepime teikiamų paaiškinimų, bankas neneigia pareiškėjos nurodytos aplinkybės, kad ginčijamos mokėjimo operacijos buvo patvirtintos ne pareiškėjos turimame ir jos naudojamame (valdomame) mobiliajame telefone su pačios pareiškėjos susikurta ir turima „Smart-ID“ tapatybės patvirtinimo priemone (t. y. pareiškėjos mobiliajame telefone esančia pareiškėjos vardu sukurta „Smart-ID“ paskyra), o per trečiųjų asmenų valdomame mobiliajame įrenginyje pareiškėjos vardu sukurta „Smart-ID“ paskyrą ir panaudojant būtent šios slaptažodžius, sukurtus ir žinomus tretiesiems asmenims, kurie juos galėjo panaudoti inicijuodami ir patvirtindami ginčijamas mokėjimo operacijas, pačiai pareiškėjai apie tai nežinant ir neišreiškus savo valios bei sutikimo dėl ginčijamų mokėjimo operacijų.

Analizuojamų aplinkybių kontekste svarbu įvertinti ir tai, ar pareiškėja, kaip ji pati pripažįsta kreipimesi į Lietuvos banką, suvedama „Smart-ID“ paskyros PIN2 kodą, galėjo suprasti, kad atlieka veiksmus, kurie gali lemti tam tikras teises pasekmes, kaip šiuo atveju – mokėjimo priemonės praradimą. Banko Taisyklių 2 priedo 11 punkte nėra įvardyta, kurio „Smart-ID“ paskyros PIN kodo (PIN1 ar PIN2) suvedimas banko ir pareiškėjos santykiuose yra laikytinas sutikimu mokėjimo operacijai iš pareiškėjos banko sąskaitos atlikti (mokėjimui mokėjimo kortele atlikti) arba, kad „Smart-ID“ paskyros PIN kodo (PIN1 ar PIN2) suvedimas naudotinas siekiant atlikti veiksmus, susijusius su turima tapatybės patvirtinimo priemone (taigi, pačia „Smart-ID“ paskyra mobiliajame įrenginyje), ir (ar) jos pakeitimu. Ši informacija plačiau aprašoma 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“ nurodoma, 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.“ Vis dėlto nagrinėjamu atveju būtina įvertinti tai, kad pareiškėja, kaip ji pati teigia kreipimesi, savo kortelės duomenis ir prisijungimo prie interneto banko duomenis tretiesiems asmenims atskleidė ir, paprašyta trečiųjų asmenų, suvedė savo „Smart-ID“ paskyros PIN2 kodą, tikėdama, kad jie, kaip prisistatė pareiškėjai, yra banko darbuotojai ir šie duomenys buvo reikalingi tam, kad banko darbuotojais prisistatę tretieji asmenys galėtų prisijungti prie pareiškėjos interneto banko ir užkirsti kelią (sustabdyti) galimai neteisėtą bandymą nurašyti lėšas iš pareiškėjos banko sąskaitos.

Vadinasi, pagal abiejų ginčų šalių neginčijamas aplinkybes ir remiantis ginčo byloje turimais įrodymais – aplinkybe, kad ginčijamų mokėjimo operacijų atlikimo dieną pareiškėjos vardu „Smart-ID“ paskyra buvo sukurta ir kitame mobiliajame įrenginyje, kuris nepriklauso pareiškėjai ir nėra jos naudojamas<sup>5</sup>, ir naudojantis šia paskyra, pagal šalių neginčijamas aplinkybes, galėjo būti patvirtintos (autorizuotos) ginčijamos mokėjimo operacijos, galima daryti prielaidą, kad ginčijamos mokėjimo operacijos buvo inicijuotos ir patvirtintos ne pačios pareiškėjos, o trečiųjų asmenų, nors ir atitiko pareiškėjos ir banko sutartą sutikimo mokėjimo operacijoms kortele davimo formą ir tvarką. Taigi, banko teiginio, kad pati pareiškėja išreiškė savo valią ir sutikimą ginčijamoms mokėjimo operacijoms šalių sutarta forma ir tvarka, nepatvirtina ginčo nagrinėjimo metu nustatytos aplinkybės ir ginčo byloje esantys įrodymai. Lietuvos banko vertinimu, vertinti pareiškėjos ginčijamų mokėjimo operacijų kaip autorizuotų – atliktų esant pačios pareiškėjos sutikimui (kaip tai suprantama Mokėjimų įstatymo 29 straipsnio 1 dalies kontekste), nėra pakankamo pagrindo, todėl šio ginčo nagrinėjimo metu Lietuvos bankas daro išvadą, kad pareiškėjos ginčijamos mokėjimo operacijos laikytinos neautorizuotomis.

*Dėl neautorizuotų mokėjimo operacijų pasekmių ir pareiškėjos teisės į ginčijamų mokėjimo operacijų sumų 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

<sup>5</sup> Pareiškėjos nurodyta aplinkybė pokalbio su banko darbuotoja metu.

šias priežastis raštu praneša priežiūros institucijai (Lietuvos bankui).

Pagal Mokėjimų įstatymo 39 straipsnio 1 dalį, mokėtojai 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 nesažiningai; 2) nuostoliai yra patirti dėl mokėjimo paslaugų teikėjo, jo darbuotojo, tarpininko, filialo ar asmenų, kuriems perduotas veiklos funkcijų valdymas, veiksmų ar neveikimo.

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

Ginčo nagrinėjimo metu buvo nustatyta, kad, prieš inicijuojant ir įvykdant ginčijamas mokėjimo operacijas, pareiškėja su ja telefonu bendravusiems tretiesiems asmenims atskleidė prisijungimo prie interneto banko duomenis (interneto banko atpažinimo (naudotojo ID) kodą) ir, jų paprašyta, suvedė savo „Smart-ID“ paskyroje PIN2, o tai įgalino trečiuosius asmenis sukurti „Smart-ID“ paskyrą kitame įrenginyje, kontroliuojamame trečiųjų asmenų, ir vėliau jų valiniais veiksmais pareiškėjos vardu inicijuoti ir patvirtinti ginčijamas mokėjimo operacijas.

Kaip minėta, pareiškėja neigia autorizavusi ginčijamas mokėjimo operacijas. Pareiškėjos teigimu, mokėjimo nurodymai įvykdyti ginčijamas mokėjimo operacijas buvo pateikti vykdyti be jos žinios ir valinių veiksmų, t. y. pačiai pareiškėjai nedavus su banku sutarta forma ir tvarka sutikimo, kad būtų vykdomi tokie mokėjimo nurodymai. Ginčo nagrinėjimo metu padaryta išvada, kad pareiškėjos ginčijamos mokėjimo operacijos laikytinos neautorizuotomis. Nors bankas su tokiu ginčijamų mokėjimo operacijų vertinimu nesutinka, vis dėlto bankas neginčija pareiškėjos nurodytos aplinkybės, kad 2021 m. gegužės 14 d. ginčijamas mokėjimo operacijas galėjo inicijuoti ir patvirtinti ne pati pareiškėja, o tretieji asmenys, kurie neteisėtai išviliojo ir pasisavino pareiškėjos jiems per neatsargumą atskleistus duomenis, būtinus prisijungti prie interneto banko sistemos, juos panaudojo naujai „Smart-ID“ paskyrai sukurti trečiųjų asmenų kontroliuojamame įrenginyje ir tą pačią dieną, naudodamiesi nauja „Smart-ID“ paskyra, inicijavo ginčijamas mokėjimo operacijas. Taigi, įvertinus pareiškėjos ir banko pateiktą informaciją apie trečiųjų asmenų neteisėtus veiksmus, dėl kurių iš pareiškėjos su kortele susietos sąskaitos banke be jos valios buvo įvykdytos ginčijamos mokėjimo operacijos, galima teigti, kad, atliekant ginčijamas mokėjimo operacijas, pareiškėjos su kortele susieta sąskaita buvo neteisėtai užvaldyta trečiųjų asmenų.

Bankas, nesutikdamas kompensuoti pareiškėjos nuostolių, susijusių su ginčijamų mokėjimo operacijų įvykdymu, ne tik teigia, kad šios operacijos buvo tinkamai autorizuotos, bet ir mano, kad buvo nustatytos sąlygos vertinti pareiškėjos elgesį kaip labai neatsargų.

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. Tokiais atvejais šio straipsnio 1 dalyje nustatytas didžiausias 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 įstatymo 37 straipsnio 3 dalyje nustatyta, 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 nesažiningai 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.

Įvertinus pirmiau nurodytas Mokėjimų įstatymo nuostatas, galima teigti, kad mokėtojo mokėjimo paslaugų teikėjas gali būti visiškai atleistas nuo pareigos gražinti mokėtojui neautorizuotos mokėjimo operacijos sumą tik tuo atveju, jeigu pateikia įrodymų dėl mokėtojo sukčiavimo (nesąžiningumo arba tyčios) arba didelio neatsargumo (Mokėjimų įstatymo 37 straipsnio 3 dalis ir 39 straipsnio 3 dalis).

Pažymėtina, kad šalių ginčo dėl to, kad pareiškėja galėjo veikti nesąžiningai arba tyčia, įskaitant sukčiavimą, nėra. Tai reiškia, kad, siekiant įvertinti, ar šiuo atveju pareiškėjos atžvilgiu galėtų būti taikoma Mokėjimų įstatymo 39 straipsnio 3 dalis, būtina nustatyti, ar pareiškėjos elgesys, prarandant mokėjimo priemonę ir jos personalizuotus saugos duomenis, gali būti vertinamas kaip didelis pareiškėjos neatsargumas (aplaidumas), dėl kurio visi nuostoliai, susiję su ginčijamų mokėjimo operacijų įvykdymu, turėtų tekti pareiškėjai.

Antrosios mokėjimo paslaugų direktyvos (toliau – PSD2) preambulės 72 punkte rašoma, kad „siekiant įvertinti galimą mokėjimo paslaugų vartotojo aplaidumą ar didelį aplaidumą, reikėtų atsižvelgti į visas aplinkybes. Įtariamo aplaidumo įrodymai ir laipsnis paprastai turėtų būti vertinami pagal nacionalinę teisę. Tačiau nors aplaidumo sąvoka reiškia, kad pažeidžiamas įsipareigojimas elgtis rūpestingai, didelis aplaidumas turėtų reikšti daugiau nei vien aplaidumą ir apimti labai nerūpestingą elgesį; pavyzdžiui, tai būtų mokėjimo operacijos autorizavimui naudojamų saugumo požymių laikymas prie mokėjimo priemonės atviru ir trečiosioms šalims lengvai atskleidžiamu formatu.“

Pažymėtina, kad didelio neatsargumo sąvoka plėtojama Lietuvos Aukščiausiojo Teismo praktikoje. Kasacinis teismas yra išaiškinęs, kad „didelis neatsargumas kaip kaltės forma pasireiškia neprotingu arba išskirtiniu rūpestingumo nebuvimu, kai asmuo nėra tiek rūpestingas, kiek akivaizdžiai būtina esamomis aplinkybėmis.“<sup>6</sup>

Lietuvos bankas, siekdamas nustatyti, ar pareiškėjos elgesys, bendraujant su trečiaisiais asmenimis ir atskleidžiant jiems savo mokėjimo priemonių personalizuotus saugumo duomenis, gali būti laikomas dideliu neatsargumu, vertino: pačios pareiškėjos elgesį bendraujant su trečiaisiais asmenimis, trečiųjų asmenų pasitelktas priemonės neteisėtu būdu išvilioti iš pareiškėjos jai priklausančių mokėjimo priemonių personalizuotus saugumo duomenis, taip pat banko veiksmus, kurių jis prevenciškai ėmėsi ir imasi tam, kad supažindintų pareiškėją su sukčiavimo elektroninėje erdvėje rizikomis bei tapatybės 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 ir perduoti mokėjimo priemonės personalizuotus saugos duomenis tretiesiems asmenims.

Elektroninėje erdvėje nusikalstamas veikas vykdančias asmenys (sukčiai) neretai pasitelkia įvairius būdus (tiek bendravimo, tiek klaidingos (suklastotos) informacijos pateikimo) tam, kad neteisėtu būdu įtikintų vartotoją atskleisti savo mokėjimo priemonių personalizuotus saugumo duomenis ir juos panaudodami įvykdytų mokėjimo operacijas, kurių pats vartotojas neautorizuoja ir savo valinių veiksmų tokioms operacijoms įvykdyti neišreiškia, kartais nežinodamas net apie tokių operacijų inicijavimo aplinkybę. Sprendžiant iš ginčo byloje esančių duomenų (pareiškėjos paaiškinimų dėl bendravimo su jai skambinusiomis trečiaisiais asmenimis aplinkybių, banko darbuotojos ir pareiškėjos pokalbių įrašų), pareiškėjos ir trečiųjų asmenų (sukčių) telefoninių pokalbių<sup>7</sup> metu tretieji asmenys, manipuliudami pareiškėjos baime prarasti banko sąskaitoje esančias lėšas, įtikinamai sukūrė emocinę aplinką, kurioje lengvai pažeidžiamas asmens (šiuo atveju – pareiškėjos) budrumas, t. y. tretieji asmenys manipuliudami pareiškėjos pažeidžiamumu, taigi, apribota galimybe itin atidžiai ir rūpestingai vertinti pateiktą informaciją ir prašymą nurodyti tik pareiškėjai žinotinus duomenis, įtikino pareiškėją atskleisti savo mokėjimo priemonių personalizuotus saugumo duomenis, kuriuos neteisėtu būdu panaudojo naujai „Smart-ID“ paskyrai sukurti ir ginčijamoms mokėjimo operacijoms įvykdyti.

Nors bankas teigia, kad ginčijamos mokėjimo operacijos buvo tinkamai autorizuotos, nes jos buvo patvirtintos šalių sutarta forma ir tvarka, bankas vis dėlto, kaip minėta, papildomai nurodo, kad, jo vertinimu, pareiškėja, bendraudama su trečiaisiais asmenimis, elgėsi itin neatsargiai (nerūpestingai) – taigi, sukčiai pareiškėjos mokėjimo priemonę ir jos personalizuotus saugos duomenis pasisavino tik dėl to, kad pareiškėjos elgesys buvo labai neatsargus. Banko teigimu, pareiškėjos itin neatsargus elgesys, pasireiškęs kortelės duomenų,

<sup>6</sup> Lietuvos Aukščiausiojo Teismo 2017 m. balandžio 13 d. nutartis civilinėje byloje Nr. e3K-3-180-378/2017, 29 punktas.

<sup>7</sup> Ginčo nagrinėjimo metu nustatytais duomenimis, pareiškėjos ir trečiųjų asmenų pokalbių buvo ne vienas.



interneto banko atpažinimo kodo atskleidimu kitiems asmenims, taip pat „Smart-ID“ paskyros PIN 1 ir PIN 2 kodų suvedimu, lėmė tai, kad pareiškėjos vardu buvo sukurta nauja „Smart-ID“ paskyra (kaip pareiškėjos tapatybės patvirtinimo priemonė) kitame mobiliajame įrenginyje, kortelė buvo registruota *TransferGo* interneto svetainėje, ginčijamos mokėjimo operacijos buvo įvykdytos, o jų lėšos nurašytos iš pareiškėjos su kortele susietos sąskaitos. Kaip nurodo bankas, didelį pareiškėjos neatsargumą patvirtina ir pačios pareiškėjos teiginiai, kuriais ji kreipimesi pripažino, kad suvedė „Smart-ID“ paskyros PIN2 kodą, taip pat pareiškėjos teiginiai banko darbuotojos ir pareiškėjos telefoninio pokalbio metu, kad pareiškėja padiktavo interneto banko atpažinimo kodą (galimai ir kortelės duomenis) kitiems asmenims. Bankas atkreipia dėmesį, kad *TransferGo* dokumentuose pateiktas kortelės Nr. „(duomenys neskelbtini)“ interneto banke yra atvaizduojamas kitaip: „(duomenys neskelbtini)“ (interneto banko išrašė nurodyta: „(duomenys neskelbtini)“), o tai, banko vertinimu, reiškia, kad kortelės duomenų informacija negalėjo būti atskleista kitiems asmenims, tik prisijungus prie pareiškėjos interneto banko paskyros, taip pat šios informacijos nepakaktų kortelės registracijai *TransferGo* interneto svetainėje (reikalingas visas 16 skaitmenų kortelės numeris, CVC kodas, kortelės galiojimo laikas), todėl šiuos duomenis turėjo atskleisti pati pareiškėja tretiesiems asmenims. Banko vertinimu, pareiškėja nesilaikė elementarių saugumo reikalavimų ir Mokėjimų įstatymo 34 straipsnyje aptartų mokėjimo paslaugų vartotojo pareigų – naudojosi mokėjimo priemone ne pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas. Taigi, bankas mano, kad buvo nustatytos sąlygos pareiškėjos elgesį vertinti kaip labai neatsargų, nes pareiškėja tretiesiems asmenims atskleidė savo mokėjimo priemonių personalizuotus saugumo duomenis, taip pažeisdama savo, kaip mokėjimo paslaugų vartotojos, pareigas. Vertinant tokius banko teisinius argumentus ir išvadas, vis dėlto, būtina pažymėti, kad pirmiau minėtų Mokėjimų įstatymo nuostatų analizė leidžia daryti išvadą, kad mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai tik tuo atveju, jei išpildomos abi sąlygos. t. y. mokėtojas ne tik neįvykdo vienos ar kelių jam Mokėjimų įstatyme nustatytų pareigų, bet ir padaro tai elgdamasis nesąžiningai arba tyčia ar būdamas labai neatsargus.

Lietuvos bankas neturi pakankamai patikimų įrodymų patvirtinančių arba paneigiančių banko nurodytus teiginius dėl kortelės duomenų (numerio) atskleidimo tretiesiems asmenims, tokios aplinkybės kreipimesi į Lietuvos banką nepatvirtina ir pati pareiškėja. Vis dėlto pareiškėja, kaip minėta, tiek pretenzijoje bankui, tiek telefoninių pokalbių su banko darbuotoja metu, tiek ir kreipimesi į Lietuvos banką pripažino, kad tretiesiems asmenims atskleidė interneto banko atpažinimo (naudotojo ID) kodą ir savo turimame mobiliajame įrenginyje, trečiųjų asmenų paprašyta, kartą suvedė „Smart-ID“ paskyros PIN2 kodą. Taigi, pareiškėja pripažino, kad tretiesiems asmenims atskleidė savo personalizuotus saugumo duomenis, o juos, kaip vėliau paaiškėjo, tretieji asmenys panaudojo pareiškėjos vardu naujai „Smart-ID“ paskyrai sukurti būtent trečiųjų asmenų kontroliuojamame galiniame įrenginyje ir iš ten pareiškėjos vardu inicijuoti ir patvirtinti ginčijamas mokėjimo operacijas savo naudai.

Vertinant pareiškėjos elgesį ir atsakomybės laipsnį dėl mokėjimo priemonės praradimo ir neautorizuotų operacijų įvykdymo, atsižvelgtina ir į tai, kad, kaip minėta pirmiau, banko cituojamų Taisyklių 2 priedo 11 punkte nėra įvardyta, kurio „Smart-ID“ paskyros PIN kodo (PIN1 ar PIN2) suvedimas banko ir pareiškėjos santykiuose yra laikytinas sutikimu mokėjimo operacijai iš pareiškėjos banko sąskaitos atlikti (mokėjimui kortele atlikti) davimu ar kad „Smart-ID“ paskyros PIN kodo (PIN1 ar PIN2) suvedimas naudotinas siekiant atlikti veiksmus, susijusius su turima tapatybės patvirtinimo priemone (taigi, pačia „Smart-ID“ paskyra mobiliajame įrenginyje), ir (ar) jos pakeitimu. Pareiškėjos turimos tapatybės patvirtinimo priemonės „Smart-ID“ tiek PIN1, tiek PIN2 kodų suvedimo, panaudojimo reikšmė nėra atskleista ir pareiškėjos bei banko Interneto banko sutartį sudarančio viešai skelbiamo Paslaugų interneto banke teikimo sąlygų aprašo nuostatose. Tokia informacija plačiau atskleidžiama tik banko interneto svetainėje adresu <https://www.seb.lt/privatiems/el-bankininkyste/paslaugos-internetu/prisijungimo-priemones-smart-id-m-parasas>. Tai leidžia daryti prielaidą, kad pareiškėjai galėjo būti ir nežinoma aplinkybė, jog, suvedant PIN2 kodą, tokiu veiksmu gali būti duotas sutikimas sukurti naują „Smart-ID“ paskyrą kitame galiniame įrenginyje.

Būtina pažymėti ir tai, kad ginčo byloje nėra ir jokių įrodymų, kokią informaciją pareiškėja matė savo mobiliojo telefono ekrane tuo metu, kai *de facto* „Smart-ID“ paskyros PIN2 kodo suvedimu patvirtino naujos šios tapatybės patvirtinimo priemonės paskyros sukūrimą trečiųjų asmenų kontroliuojamame galiniame įrenginyje. Taigi, ginčo byloje nėra duomenų ir juos pagrindžiančių įrodymų, kad pareiškėja savo mobiliajame įrenginyje esančioje programėlėje „Smart-ID“ suveddama PIN2 kodą matė, jog šiuo veiksmu tvirtina naujos „Smart-



ID" paskyros sukūrimą, kaip ir nėra jokių duomenų, kokią ir ar apskritai kokią nors papildomą informaciją pareiškėja matė programėlės „Smart-ID“ languose, prašančiuose suvesti PIN1 ir PIN2 kodus.

Bankas atsiliepime, be kita ko, nurodo, kad, siekdamas tinkamai informuoti mokėjimo paslaugų vartotojus, savo interneto svetainėje skelbia informaciją apie suaktyvėjusius sukčius, taip pat nuolat perspėja ir ragina savo klientus būti labai atidžius, niekada neatskleisti, nevesti savo asmens, mokėjimo kortelių ir interneto banko prisijungimo duomenų trečiųjų asmenų prašymu, kritiškai tokius prašymus įvertinti. Vis dėlto tokie banko teiginiai niekaip nepagrindžia aplinkybės, kad pareiškėja buvo banko tinkamai informuota apie naudojimosi tapatybės patvirtinimo priemone „Smart-ID“ ypatumus ir PIN kodų „Smart-ID“ programėlėje suvedimo reikšmę bei pasekmes, taip pat ir to, kad pareiškėja buvo informuota ir žinojo apie tokio pobūdžio sukčiavimo atakas, kokia buvo įvykdyta ir prieš pačią pareiškėją, t. y. kad sukčiai, išvilioję iš pareiškėjos jos mokėjimo priemonių personalizuotus saugumo duomenis, gali sukurti naują „Smart-ID“ paskyrą nuotoliniu būdu jų kontroliuojamame galiniame įrenginyje ir iš ten be mokėtojo (šiuo atveju – pareiškėjos) valios ir žinojimo patvirtinti lėšų pervedimo operacijas<sup>8</sup>. Vystantis ir tobulėjant technologijoms, vystomi ir sukčiavimo būdai bei priemonės, sudėtingėja pačios sukčiavimo atakos, todėl tam 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 kompleksiško 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. Dėl šios priežasties 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. Kaip minėta, konkrečių duomenų ir juos patvirtinančių įrodymų, kad bankas būtų aktyviai vykdęs informavimo pareigą ir pareiškėją būtų tinkamai informavęs apie atitinkamas sukčiavimo atakas ir su tuo susijusias rizikas, ginčo nagrinėjimo metu nenustatyta.

Vertinant pareiškėjos elgesį ir sprendžiant dėl jos neatsargumo laipsnio, būtina atsižvelgti į tai, kad pareiškėjai skambinę treieji asmenys, prisistatę banko darbuotojais, savo iniciatyva nuo pat pradžių bendravo su pareiškėja rusų kalba. Pareiškėja pokalbio su banko darbuotoja metu paaiškino, kad skambinusio asmens pasiteiravo, kodėl su ja yra bendraujama rusų kalba, o skambinęs asmuo, pareiškėjos teigimu, jai nurodęs, kad pareiškėjos kliento anketoje yra nurodyta, kad ji gali bendrauti tiek lietuvių, tiek rusų kalbomis, todėl pareiškėja toliau tęsė pokalbį ir bendravimą su trečiaisiais asmenimis. Vis dėlto būtina atkreipti dėmesį, kad Lietuvoje veikiančių finansinių paslaugų teikėjų paslaugos teikiamos valstybine kalba ir tik šalims susitarus bei vartotojui pageidaujant vartotojai gali būti aptarnaujami (su jais bendraujama) ir kita nei valstybinė kalba. Tad trečiųjų asmenų, prisistačiusių banko darbuotojais, bendravimas rusų kalba, pareiškėjai tokio pageidavimo pačiai neišreiškus, turėjo sukelti įtarimų dėl skambinusių asmenų tapatybės. Ir nors pirmiau aptarta aplinkybė iš tiesų sukėlė įtarimų, pareiškėja ne tik su jai iš skirtingų telefono numerių skambinusiaisiais rusakalbiais asmenimis bendravo net keletą kartų<sup>9</sup> (taigi, turėjo pakankamai galimybių laiko prasme suvokti prašomų atlikti veiksmų pobūdį ir galimas to pasekmes), bet ir besąlygiškai patikėjo trečiųjų asmenų pateiktais paaiškinimais, o vėliau, jų paprašyta, ir atskleidė jiems tam tikrus personalizuotus saugumo duomenis. Šie duomenys, kaip matyti iš ginčo nagrinėjimo metu nustatytų aplinkybių, vėliau įgalino trečiuosius asmenis sukurti naują „Smart-ID“ paskyrą pareiškėjos vardu trečiųjų asmenų kontroliuojamame galiniame įrenginyje, inicijuoti ir įvykdyti ginčijamas mokėjimo operacijas.

Kaip jau minėta pirmiau, Mokėjimų įstatymo 34 straipsnyje reglamentuojama viena iš mokėjimo paslaugų vartotojo, turinčio teisę naudotis mokėjimo priemone, pareigų – naudotis

<sup>8</sup> Atsiliepime bankas nurodo, kad, siekdamas tinkamai informuoti mokėjimo paslaugų vartotojus, savo interneto svetainėje skelbia informaciją apie suaktyvėjusius sukčius, nuolat perspėja ir ragina savo klientus būti labai atidžius, niekada neatskleisti, nevesti savo asmens, mokėjimo kortelių ir interneto banko prisijungimo duomenų trečiųjų asmenų prašymu. Vis dėlto, pagrįsdamas šiuos teiginius, bankas atsiliepime pateikia nuorodą tik apie saugaus atsiskaitymo internetu eigą ir tvarką (<https://www.seb.lt/privatiems/mokejimo-korteles/kaip-saugiai-internetu-atsiskaityti-mokejimo-kortele>).

<sup>9</sup> Pagal ginčo byloje esančius duomenis (atsiliepime, pareiškėjos ir banko darbuotojos telefoninių pokalbių įrašuose nurodyta informacija), pareiškėjai rusakalbiai asmenys skambino iš skirtingų telefono numerių (tel. Nr.: (duomenys neskelbtini), (duomenys neskelbtini), (duomenys neskelbtini)) ir ji pripažino su šiais asmenimis bendravusi kelis kartus.

mokėjimo priemone pagal mokėjimo priemonės išdavimą ir naudojimą reglamentuojančias sąlygas. Banko 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.

Neabejotina, kad aptartas pareiškėjos elgesys, galiausiai nulėmęs naujos tapatybės patvirtinimo priemonės pareiškėjos vardu sukūrimą ir neautorizuotų mokėjimo operacijų įvykdymą, negali būti vertinamas atitinkančiu pareiškėjai, kaip mokėjimo paslaugų vartotojai, Mokėjimų įstatyme bei šalių sudarytose Interneto banko sutartyje ir Kortelės sutartyje (jas sudarančiuose dokumentuose) nustatytus įpareigojimus išsaugoti išduotų mokėjimo priemonių personalizuotų saugumo duomenų konfidencialumą. Kita vertus, pirmiau konstatuota aplinkybė savaime nesuponuoja išvados, kad pareiškėjos neatsargus elgesys, vertintinas kaip didelis neatsargumas, t. y. aplinkybė, kad pareiškėja pažeidė savo pareigą tinkamai apsaugoti turimų mokėjimo priemonių personalizuotų saugumo duomenų konfidencialumą, savaime nereiškia, jog jos elgesys buvo ne tik neatsargus, bet ir toks aplaidus, kad sukeltų pareiškėjai Mokėjimų įstatymo 39 straipsnio 3 dalyje nurodytas pasekmes, dėl ko visi nuostoliai dėl neautorizuotų mokėjimo operacijų turėtų tekti būtent pareiškėjai.

Ginčo nagrinėjimo metu Lietuvos bankas, siekdamas tinkamai įvertinti tiek pareiškėjos elgesį – atsakomybę dėl naujos „Smart-ID“ paskyros pareiškėjos vardu sukūrimo ir įvykdytų neautorizuotų mokėjimo operacijų, tiek pačios sukčiavimo atakos pobūdį ir trečiųjų asmenų veikimo aplinkybes, kreipėsi į ginčo šalis, prašydamas pateikti papildomus paaiškinimus.

Pateikdama papildomus paaiškinimus, pareiškėja nurodė, kad, bendraudama su trečiaisiais asmenimis, prisistačiusiais banko darbuotojais, į savo mobilųjį telefoną gavo rusų kalba, tačiau lietuviškais rašmenimis parašytą SMS žinutę apie naujos „Smart-ID“ paskyros sukūrimą.

Bankas, atsakydamas į Lietuvos banko prašymą pateikti papildomus duomenis dėl to, ar ir kaip pareiškėja buvo informuota apie naujos „Smart-ID“ paskyros pareiškėjos vardu sukūrimą, nurodė, kad, iš „SK ID solutions AS“ gautais duomenimis, minėta bendrovė siuntė 1) ranešimą lietuvių kalba el. pašto adresu (*duomenys neskelbtini*), t. y. el. pašto adresu, kuris ir pareiškėjos kreipimesi į Lietuvos banką nurodytas kaip jos el. pašto adresas. Pažymėtina, kad ginčo nagrinėjimo metu pareiškėja taip pat patvirtino, kad į savo el. paštą gavo pranešimą, informuojantį ją apie naujos „Smart-ID“ paskyros sukūrimą, tačiau el. paštą pasitikrino tik ginčijamų mokėjimo operacijų įvykdymo dienos pabaigoje; 2) SMS pranešimą anglų kalba, jo tekstas „Congratulations X! Your Smart-ID account is ready to use. Enjoy! More information: [www.smart-id.com/welcome](http://www.smart-id.com/welcome)“. Šis pranešimas buvo siųstas telefono numeriu (*duomenys neskelbtini*). Būtina atkreipti dėmesį, kad šis telefono numeris nėra nurodytas pareiškėjos kreipimesi kaip jos telefono numeris, duomenų ir juos pagrindžiančių įrodymų, kad minėtas telefono numeris būtų sietinas su pareiškėja, taip pat nepateikė ir bankas. Dėl šios priežasties preziumuotina, kad „SK ID solutions AS“ SMS pranešimas anglų kalba, informuojantis apie naujos „Smart-ID“ paskyros sukūrimą, buvo išsiųstas tretiesiems asmenims (į jų mobilųjį įrenginį), neteisėtai pareiškėjos vardu būtent šiame mobiliajame įrenginyje sukūrusiems naują „Smart-ID“ paskyrą pareiškėjos vardu. Bankas taip pat nurodė, kad pareiškėjai pats papildomai siuntė SMS pranešimą telefono numeriu (*duomenys neskelbtini*) (šį telefono numerį pareiškėja yra pateikusi bankui kaip kontaktinį telefono numerį, taip pat nurodžiusi ir kreipimesi į Lietuvos banką kaip savo telefono numerį), kuriuo bankas informavo, kad kuriama „Smart-ID“ paskyra: „Dobryj denj! Profilj Smart-ID Basic registruetsja ot Vashego imeni v banke SEB. Jesli Vy ne nachinali registracii, pozvonite nam (*duomenys neskelbtini*). Bank SEB“. Kaip minėta pirmiau, remiantis pareiškėjos papildomais paaiškinimais ir kartu su jais pateiktais duomenimis, pareiškėja neneigia ginčijamų mokėjimo operacijų įvykdymo dieną, bendravimo (telefoninių pokalbių) su trečiaisiais asmenimis metu, į savo telefoną gavusi iš banko SMS pranešimą, informuojantį ją apie naujos „Smart-ID“ paskyros sukūrimą. Pareiškėja savo paaiškinimuose nurodo, kad gauta žinutė jai sukėlė įtarimų, nes buvo parašyta lietuviškais rašmenimis, tačiau rusų kalba. Pareiškėjai pasiteiravus su ja bendravusių trečiųjų asmenų, kaip reikėtų reaguoti į gautą (pareiškėjos teigimu, įtartina) pranešimą, pareiškėjai buvo patarta nekreipti dėmesio, tretiesiems asmenims nurodžius, kad žinutė buvo išsiųsta „žuliku“. Pareiškėja papildomuose paaiškinimuose pripažino, kad patikėjo trečiųjų asmenų, nes tuo metu manė, kad jie yra banko darbuotojai, paaiškinimais, kad žinutė atsiųsta sukčių, ir papildomų veiksmų (reagavimo) dėl šios žinutės, kad išsiaiškintų, ar joje nurodyta informacija yra teisinga, kaip ir dėl įtartinais pasirodžiusių trečiųjų rusakalbių asmenų skambučių, vėlgį nesiėmė. Įvertintina ir tai, kad banko

siųstas SMS pranešimas, informuojantis apie naujos „Smart-ID“ paskyros sukūrimą, pačiai pareiškėjai, jos teigimu, atrodė įtartinas, neįprastas, nes buvo parašytas rusų kalba, tačiau lietuviškais rašmenimis. Bankas kartu su papildomais duomenimis nepateikė jokių paaiškinimų, kodėl pareiškėjai skirta SMS žinutė apie naujos „Smart-ID“ paskyros sukūrimą buvo siųsta rusų kalba, tačiau lietuviškais rašmenimis, nors, kaip matyti iš pareiškėjos kartu su papildomais paaiškinimais pateiktų jos mobiliojo telefono ekrano nuotraukų, kita banko pareiškėjai siųsta SMS žinutė, informuojanti apie kredito paraiškos užpildymą, buvo siųsta lietuvių kalba. Vis dėlto, kadangi pati SMS žinutė pareiškėjai pasirodė įtartina, kaip ir iš pradžių patys jai paskambinę ir su pareiškėja rusų kalba bendravę tretieji asmenys, manytina, kad pareiškėja, būdama pakankamai atidi ir rūpestinga, galėjo imtis papildomų veiksmų tam, kad tinkamai įvertintų jai įtartinas pasirodžiusias aplinkybes – tiek iš banko gauto SMS pranešimo turinį, tiek ir patį bendravimą su trečiaisiais asmenimis telefonu rusų kalba bei jų prašymus atskleisti personalizuotus saugumo duomenis, tačiau to nepadarė.

Sprendžiant dėl pareiškėjos neatsargumo laipsnio, į aptartinių aplinkybių apimtį įtrauktinas ir faktas, kad tretieji asmenys, bendraudami su pareiškėja, pasinaudojo pareiškėjos baime prarasti banko sąskaitoje esančias lėšas ir, manipuliudami šia baime, įtikino ją atskleisti savo personalizuotus saugos duomenis ir kartą suvesti savo tapatybės patvirtinimo priemonės „Smart-ID“ PIN2 kodą: sprendžiant iš pareiškėjos ir banko darbuotojos darbo pokalbio įrašų, tretieji asmenys vieno iš pokalbių su pareiškėja metu klausė, ar pareiškėja pažįsta Y.Y. ir ar ji iš tiesų siekia šiam asmeniui pervesti 130 Eur į sąskaitą, esančią mokėjimo įstaigoje Latvijos Respublikoje. Siekiant atšaukti pateiktą mokėjimo nurodymą, pareiškėjos buvo prašoma atskleisti tam tikrus duomenis<sup>10</sup> ir kartą suvesti programėlės „Smart-ID“ PIN2 kodą. Manytina, kad toks trečiųjų asmenų elgesys, bendravimo būdas, ypač atsižvelgiant į tai, kad, kaip minėta pirmiau, pareiškėjos tapatybės patvirtinimo priemonės „Smart-ID“ tiek PIN1, tiek PIN2 kodų suvedimo, jų panaudojimo reikšmė nėra atskleista pareiškėjos ir banko sudarytoje Interneto banko sutartyje ar ją sudarančiuose dokumentuose, tad „Smart-ID“ paskyros PIN2 kodo suvedimas pareiškėjos galėjo būti ir nesuvoktas kaip labai neatsargus veiksmas.

Įvertintina ir tai, kad trečiųjų asmenų įvykdyta sukčiavimo ataka buvo sofistikuota – įvykdyta pasinaudojant egzistuojančia technine galimybe sukurti naują tapatybės patvirtinimo priemonės „Smart-ID“ paskyrą nuotoliniu būdu kitame mobiliajame įrenginyje. Iš ginčo nagrinėjimo metu nustatytų aplinkybių matyti, kad pareiškėja manipuliatyviai, neteisėtu būdu buvo įtikinta atskleisti savo personalizuotus saugos duomenis (interneto banko naudotojo atpažinimo kodą), o vėliau ir suvesti „Smart-ID“ paskyros PIN2 kodą. Ginčo nagrinėjimo metu nustatyta, kad tokiu veiksmu buvo patvirtinta nauja sukurta „Smart-ID“ paskyra, ir ją naudojantis, pačiai pareiškėjai nedalyvaujant, t. y. neinicijuojant ir nepatvirtinant (neautorizuojant), ir neišreiškiant jokių kitų valinių veiksmų, buvo įvykdytos ginčijamos mokėjimo operacijos, apie jų inicijavimo ir įvykdymo faktą pareiškėjai net nežinant iki atitinkamo banko pranešimo, kai pareiškėja buvo informuota, kad, įvykus sukčių atakai, neautorizuotų mokėjimo operacijų iš jos sąskaitos banke vis dėlto būta. Aplinkybė, kad pareiškėja atskleidė tretiesiems asmenims tam tikrus personalizuotus saugumo duomenis ir kartą trečiųjų asmenų prašoma suvedė „Smart-ID“ paskyros PIN2 kodą, lėmė tai, kad pareiškėjos vardu buvo ne tik sukurta nauja tapatybės patvirtinimo priemonės „Smart-ID“ paskyra trečiųjų asmenų kontroliuojamame mobiliajame įrenginyje, bet ir iš pareiškėjos banko sąskaitos įvykdytos net aštuonios mokėjimo operacijos, kurias atliekant faktiškai pati pareiškėja nedalyvavo, joms savo sutikimo nedavė ir net nežinojo apie inicijavimo ir patvirtinimo aplinkybę.

Ginčo nagrinėjimo metu Lietuvos bankas taip pat paprašė banko pateikti papildomus paaiškinimus ir juos pagrindžiančius duomenis, ar, tretiesiems asmenims tvirtinant visas aštuonias ginčijamas mokėjimo operacijas iš pareiškėjos vardu sukurtos naujos „Smart-ID“ paskyros trečiųjų asmenų kontroliuojamame mobiliajame įrenginyje, pareiškėjos telefone taip pat atsirado („iššoko“) pačios pareiškėjos naudojamos tapatybės patvirtinimo priemonės „Smart-ID“ pranešimai, prašantys suvesti PIN1 kodą (tam, kad būtų prisijungta prie interneto banko paskyros) ir PIN2 kodą (tam, kad būtų patvirtinta atitinkama mokėjimo operacija). Bankas, paaiškindamas prašomas aplinkybes, pateikė iš „SK ID Solutions AS“ gautus duomenis, kad pranešimai, prašantys patvirtinti pareiškėjos prisijungimą prie interneto banko, ir

<sup>10</sup> Tiek pirmojo pokalbio su banko darbuotoja, pranešant apie galimai įvykusią sukčiavimo ataką, metu, tiek ginčo nagrinėjimo metu Lietuvos bankui pareiškėja pripažino tretiesiems asmenims atskleidusi tik savo interneto banko atpažinimo kodą ir kartą suvedusi savo mobiliajame telefone esančioje „Smart-ID“ programėlėje šios paskyros PIN2 kodą.

pranešimai, prašantys patvirtinti ginčijamas mokėjimo operacijas, pasirodė abiejuose įrenginiuose, su kuriais buvo susietos pareiškėjos vardu sukurtos „Smart-ID“ paskyros.

Vis dėlto, įvertinus banko pateiktą informaciją, būtina pažymėti, kad banko papildomai pateikti duomenys nepagrindžia aplinkybės, kad pareiškėja tikrai matė, jog jos vardu su kortele susietoje sąskaitoje buvo siekiama įvykdyti ginčijamas mokėjimo operacijas. Ginčo byloje nėra jokių duomenų, kad pareiškėjos telefone pagrindiniame ekrane turėjo automatiškai atsirasti ir tikrai atsirado („iššoko“) pačios pareiškėjos susikurtos tapatybės patvirtinimo priemonės „Smart-ID“ pranešimai, prašantys suvesti PIN1 ir PIN2 kodus<sup>11</sup>, o jei jie turėjo pasirodyti („iššokti“) – kad pareiškėja telefone tikrai matė pasirodžiusius („iššokusius“) atitinkamus pranešimus, nes tokios aplinkybės pati pareiškėja nepatvirtina. Ginčo byloje taip pat nėra duomenų, kiek laiko atsiradęs pranešimas (jei toks atsirado), prašantis suvesti PIN1 ir PIN2 kodus, galėjo būti rodomas pareiškėjos telefone (turint omenyje, kad visos ginčijamos mokėjimo operacijos buvo patvirtintos būtent iš trečiųjų asmenų kontroliuojamos pareiškėjos vardu sukurtos naujos „Smart-ID“ paskyros ir šios paskyros PIN kodai, susidedantys iš 4–5 skaitmenų, tikėtina, buvo suvesti per sekundę, daugiausia – per kelias sekundes) ir kad pareiškėja ginčijamų mokėjimo operacijų metu telefoną turėjo šalia savęs ir turėjo galimybę pranešimus pamatyti. Aplinkybė, kad buvo įvykdytos net aštuonios neautorizuotos mokėjimo operacijos, suponuoja išvadą, jog mažai tikėtina, kad pareiškėja galėjo matyti ir (ar) matė programėlės „Smart-ID“ pranešimus, prašančius suvesti PIN2 kodą aštuonis kartus, tačiau į tai visiškai nereagavo ir būtų nesupratusi, jog bandoma neteisėtu būdu nurašyti lėšas iš jos su kortele susietos sąskaitos.

Pareiškėja banko atžvilgiu keliamą reikalavimą kompensuoti ginčijamų mokėjimo operacijų lėšas grindžia ir prielaida, kad banko pritaikytos saugumo priemonės (operacijų stebėjimo mechanizmai) buvo nepakankami, o tai patvirtina faktas, kad bankas neautorizuotų mokėjimo operacijų sumas pervedė sukčiams (t. y. bankas pervedė ginčijamų mokėjimo operacijų sumas į *TransferGo* esančią sąskaitą, iš kurios vėliau visos, išskyrus paskutinę, ginčijamų mokėjimo operacijų lėšos pervestos į trečiųjų asmenų, neteisėtu būdu pasisavinusių pareiškėjos mokėjimo priemonę ir jos vardu patvirtinusių ginčijamas mokėjimo operacijas, sąskaitą užsienio banke).

2017 m. lapkričio 27 d. 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)<sup>12</sup>, ir kuris priimtas siekiant užtikrinti, kad elektroniniu būdu siūlomos mokėjimo paslaugos būtų teikiamos saugiai, įdiegiant technologijas, kuriomis galima užtikrinti saugų vartotojo autentiškumo patvirtinimą ir kuo labiau sumažinti sukčiavimo riziką, 2 straipsnyje nustatyti bendrieji autentiškumo patvirtinimo reikalavimai, kurių tinkamą įvykdymą turi užtikrinti mokėjimo paslaugų teikėjai. Pagal minėto straipsnio nuostatas, mokėjimo paslaugų teikėjai įdiegia operacijų stebėjimo mechanizmus, leidžiančius jiems aptikti neautorizuotas ar nesąžiningas mokėjimo operacijas, kad galėtų įgyvendinti saugumo priemones, nurodytas Reglamento 1 straipsnio a ir b punktuose. Tie mechanizmai yra grindžiami mokėjimo operacijų analize, kurią atliekant atsižvelgiama į mokėjimo paslaugų vartotojui būdingus elementus įprastu būdu naudojant personalizuotus saugumo požymius (1 dalis). Mokėjimo paslaugų teikėjai užtikrina, kad operacijų stebėjimo mechanizmais būtų atsižvelgiama bent į kiekvieną iš šių rizika grindžiamų veiksnių: a) neteisėtai sužinotų ar pavogtų autentiškumo nustatymo elementų sąrašus; b) kiekvienos mokėjimo operacijos sumą; c) žinomus sukčiavimo scenarijus teikiant mokėjimo paslaugas; d) užkrėtimo kenkimo programine įranga požymius per bet kurį autentiškumo patvirtinimo procedūros seansą; e) tais atvejais, kai priegos prietaisą arba programinę įrangą suteikė mokėjimo paslaugų teikėjas, mokėjimo paslaugų vartotojui suteikto priegos prietaiso arba programinės įrangos naudojimo ir netinkamo jų naudojimo žurnalą. Be to, remiantis Reglamento nuostatomis, autentiškumo patvirtinimo procedūra turėtų apimti operacijų stebėjimo mechanizmus, kuriais būtų galima nustatyti mėginimus pasinaudoti mokėjimo paslaugų vartotojo personalizuotais saugumo požymiais, kurie buvo prarasti, pavogti arba neteisėtai pasisavinti, ir užtikrinti, kad mokėjimo

<sup>11</sup> Priežastys, kodėl telefone, kuriame instaliuota „Smart-ID“ programėlė, kaip tapatybės patvirtinimo priemonė, neatsiranda automatiniai pranešimai, gali būti labai įvairios, plačiau žr.: <https://www.smart-id.com/lt/pagalba/duk/smart-id-programeles-pranesimai/nematau-smart-id-naujienu-pranesimu-savo-telefone> (žr. „Negaunu „Smart-ID“ pranešimų įrenginiuose su „iOS“ operacine sistema“, „Nematau „Smart-ID“ naujienu pranešimų savo telefone“, „Kaip naudoti „Smart-ID“, jei išmanusis įrenginys negauna pranešimų?“ ir kt.).

<sup>12</sup> <https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32018R0389&from=EN>

paslaugų vartotojas, įprastu būdu nurodęs personalizuotus saugumo požymius, būtų teisėtas vartotojas ir kaip toks išreikštų savo sutikimą pervesti lėšas ir gauti informaciją apie savo sąskaitą<sup>13</sup>.

Lietuvos banko prašymu bankas, pateikdamas papildomus paaiškinimus dėl taikomų saugumo priemonių, nurodė, kad yra įgyvendinęs ir taikė pareiškėjos inicijuotoms operacijoms griežto kliento autentiškumo patvirtinimo saugumo priemones, kaip tai nustatyta Reglamento ir Mokėjimų įstatymo nuostatose. Banko vertinimu, jo taikomos griežto kliento autentiškumo patvirtinimo saugumo priemonės yra veiksmingos tik tada, kai mokėjimo paslaugų vartotojas (nagrinėjamu atveju – pareiškėja) laikosi teisės aktuose ir šalių sudarytoje sutartyje nustatytų reikalavimų, susijusių su personalizuotų saugumo požymių saugojimu, neatskleidimu ir kitokiu naudojimu, neatskleidžiant jų tretiesiems asmenims, ir naudojami mokėjimo paslaugomis elgdamasis atsargiai. Bankas pažymi, kad jis, kaip mokėjimo paslaugų teikėjas, šiuo atveju laiku ir tinkamai vykdė visus pirmiau nurodytų teisės aktų reikalavimus – reikalavo, kad pareiškėjai atpažinti ir mokėjimo operacijai patvirtinti būtų atlikti veiksmai, atitinkantys griežto kliento autentiškumo patvirtinimo reikalavimus, o taikydamas saugesnio autentiškumo patvirtinimo procedūrą, užtikrino dinamišką pareiškėjos inicijuotų mokėjimo operacijų susiejimą su mokėjimo operacijos sumomis ir konkrečiu lėšų gavėju.

Bankas Lietuvos bankui nepateikė duomenų, ar, vykdant pareiškėjos ginčijamas mokėjimo operacijas, banke buvo įdiegti ir taikomi mokėjimo operacijų stebėjimo mechanizmai, vykdyta pareiškėjos vardu inicijuotų mokėjimo nurodymų įvykdyti ginčijamas mokėjimo operacijas analizė, taikytos kitos priemonės, kad pareiškėjos vardu iš jos su kortele susietos sąskaitos nebūtų įvykdytos pačios pareiškėjos neautorizuotos mokėjimo operacijos. Kaip matyti iš banko pateiktų paaiškinimų, bankas, siekdamas įgyvendinti Reglamento ir Mokėjimų įstatymo reikalavimus, susijusius su saugumo priemonių įgyvendinimu, taiko griežto kliento autentiškumo patvirtinimo saugumo priemones, t. y. bankas klientų inicijuotoms mokėjimo operacijoms autorizuoti taiko saugesnio autentiškumo nustatymo procedūrą. Lietuvos bankas neturi pakankamai duomenų, kad galėtų patvirtinti ar paneigti aplinkybę, jog bankas nagrinėjamu atveju ėmėsi pakankamų saugumo priemonių, vykdydamas pareiškėjos ginčijamas mokėjimo operacijas, kaip tai nustatyta Reglamento nuostatose, tačiau faktas, kad visos pareiškėjos ginčijamos mokėjimo operacijos buvo patvirtintos taikant saugesnio autentiškumo patvirtinimo procedūrą. Sutiktina su banko nurodytu teiginiu, kad saugesnio autentiškumo patvirtinimo procedūros yra veiksmingos tada, kai tinkamai laikomasi teisės aktuose ir sutartyse su banku nustatytų reikalavimų, susijusių su personalizuotų saugumo požymių saugojimu. Taip pat faktas ir neginčijama šalių aplinkybė, kad pati pareiškėja atskleidė tretiesiems asmenims su jos turimomis mokėjimo priemonėmis susijusius saugumo duomenis, kurie turėjo būti žinomi tik pareiškėjai. Taigi, pati pareiškėja šiuo atveju neužtikrino savo personalizuotų saugumo duomenų konfidencialumo. Toks pareiškėjos elgesys lėmė tai, kad banko taikyta saugesnio autentiškumo patvirtinimo procedūra šiuo atveju nebuvo pakankama tam, kad apsaugotų pareiškėją nuo sukčiavimo atakos ir neautorizuotos mokėjimo operacijos iš jos su kortele susietos sąskaitos nebūtų įvykdytos.

Kita vertus, aplinkybė, kad ginčijamos mokėjimo operacijos buvo patvirtintos naudojant mokėjimo operacijoms autorizuoti šalių sutartiniuose santykiuose sutartus naudoti saugesnio autentiškumo nustatymo reikalavimus, šiuo atveju, esant įrodymų, kad šalių sutarta mokėjimo operacijų saugesnio autentiškumo patvirtinimo procedūra tretieji asmenys pasinaudojo be pareiškėjos žinios ir valinių veiksmų bei sutikimo, nedaro tokių operacijų autorizuotomis, bet kartu, kaip buvo konstatuota pirmiau, ir savaime nesuponuoja išvados, kad pareiškėjos elgesys, bendraujant su trečiaisiais asmenimis ir prarandant mokėjimo priemonę (įgalinant trečiuosius asmenis sukurti naują „Smart-ID“ paskyrą), vertintinas kaip labai neatsargus.

Lietuvos bankas pažymi, kad didelis neatsargumas ar paprastas neatsargumas yra vertinamojo pobūdžio aplinkybė ir išvada dėl mokėtojo elgesio vertinimo kaip neatsargaus ar labai neatsargaus dėl neautorizuotos (-ų) mokėjimo operacijos (-ų) ar dėl mokėjimo priemonės praradimo, lėmusio neautorizuotą (-as) mokėjimo operaciją (-as), darytina kiekvienu konkrečiu atveju, įvertinus ginčo nagrinėjimo metu nustatytų individualių, specifinių aplinkybių visumą, kurią patvirtina ginčo byloje esantys įrodymai ir (arba) yra šalių neginčijamos neautorizuotos mokėjimo operacijos įvykdymo aplinkybės. Taigi, išvada dėl mokėtojo paprasto ar didelio neatsargumo, kaip vertinamojo pobūdžio aplinkybė, negali būti daroma izoliuotai, išsamiai neįvertinus viso neautorizuotų mokėjimo operacijų įvykdymo ir su juo susijusių aplinkybių

<sup>13</sup> Reglamento preambulės 1 punktą.

konteksto.

Šiuo atveju ginčo byloje esantys įrodymai ir pirmiau analizuotos ginčo nagrinėjimo metu nustatytos aplinkybės, susijusios tiek su pačios sukčiavimo atakos pobūdžiu, tiek su banko veiksmais, o svarbiausia – susijusios su pačios pareiškėjos veiksmais, net įvertinus ir tai, kad nagrinėjamo ginčo kontekste aktuali sukčiavimo ataka buvo sofistikuota ir ją pastebėti buvo būtinas pareiškėjos atidumas ir rūpestingumas, taip pat tai, kad banko veiksmai, supažindinant pareiškėją su tapatybės patvirtinimo priemonės „Smart-ID“ PIN1 ir PIN2 kodų suvedimo reikšme ir informuojant, perspėjant apie sukčiavimo grėsmes, įvertinti kaip nepakankami, vis dėlto nesudaro pagrindo vertinti pareiškėjos elgesio tik kaip neatsargaus. Vertinamų aplinkybių kontekste būtina pažymėti tai, kad pareiškėja, kaip ji pati to neneigia, bendraudama telefonu ne kartą su iš skirtingų telefono numerių jai skambinusiais rusakalbais asmenimis ir besąlygiškai jais pasitikėdama, nepatikrinusi trečiųjų asmenų nurodytos informacijos teisingumo, jiems atskleisdama savo mokėjimo priemonių personalizuotus saugumo duomenis, elgėsi itin neapdairiai ir neįvykdė jai, kaip mokėjimo paslaugų vartotojai, Mokėjimų įstatyme ir sutartyse su banku nustatytų pareigų saugoti ir niekam neatskleisti šių duomenų. Taigi, būtent ši ginčo nagrinėjimo metu konstatuota aplinkybė, t. y. kad pareiškėja neužtikrino jai išduotų mokėjimo priemonių personalizuotų saugumo duomenų konfidencialumo, elgdamsi labai neatsargiai, lėmė tai, kad tretieji asmenys įgijo galimybę sukurti naują „Smart-ID“ paskyrą pareiškėjos vardu trečiųjų asmenų kontroliuojamame mobiliajame įrenginyje ir iš ten patvirtinti jų inicijuotas ginčijamas mokėjimo operacijas. Lietuvos banko vertinimu, pirmiau aptartos aplinkybės, susijusios su pareiškėjos bendravimu su trečiaisiais asmenimis, atsižvelgus ir į pirmiau cituotą kasacinio teismo praktiką dėl didelio neatsargumo, leidžia teigti, kad pareiškėja, nesilaikydama jai, kaip mokėjimo paslaugų vartotojai, nustatytų pareigų, susijusių su mokėjimo priemonės naudojimu, nebuvo tiek atidi ir rūpestinga, kiek akivaizdžiai buvo būtina nurodytomis aplinkybėmis. Tai suponuoja išvadą, kad pareiškėjos elgesys, bendraujant su trečiaisiais asmenimis (savo saugumo duomenų atskleidimas tretiesiems asmenims), galiausiai lėmęs ir ginčijamų mokėjimo operacijų įvykdymą bei jų sumų nurašymą iš pareiškėjos sąskaitos banke, gali būti vertinamas kaip didelis pareiškėjos neatsargumas (aplaidumas), todėl visi nuostoliai, susiję su ginčijamų mokėjimo operacijos įvykdymu, turėtų tekti pareiškėjai.

Įvertinus pirmiau išdėstytą informaciją, konstatuotina, kad yra pagrindas taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį, nustatančią, kad mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai, jeigu jis juos patyrė dėl didelio neatsargumo neįvykdęs vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų, todėl, Lietuvos banko vertinimu, bankas neturi pareigos pareiškėjai gražinti neautorizuotų mokėjimo operacijų lėšų.

#### *Dėl mokėjimo nurodymų įvykdyti ginčijamas mokėjimo operacijas atšaukimo*

Pareiškėja kreipėsi teigia, kad sužinojusi apie ginčijamas mokėjimo operacijas iškart kreipėsi į banką dėl mokėjimo nurodymų šias operacijas įvykdyti atšaukimo ir tikėjosi, kad lėšos į trečiųjų asmenų sąskaitą nebus pervestos. Pareiškėja atkreipia dėmesį, kad kreipimosi į banką dėl ginčijamų mokėjimo operacijų atšaukimo metu lėšos su kortele susietoje sąskaitoje dar buvo tik rezervuotos, tačiau nenurašytos, todėl bankas, pareiškėjos vertinimu, pareiškėjos vardu pateiktus mokėjimo nurodymus įvykdyti ginčijamas mokėjimo operacijas turėjo galimybę atšaukti ir lėšų į trečiųjų asmenų sąskaitą nepervesti, tačiau to nepadarė.

Atsižvelgiant į tai, papildomai pažymėtina, kad pagal Mokėjimų įstatymo 44 straipsnio 1 dalies nuostatas, mokėjimo paslaugų vartotojas negali atšaukti mokėjimo nurodymo po to, kai jį 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 nustatytais atvejais būtinas ir gavėjo sutikimas. Mokėjimo paslaugų teikėjas gali imti komisinį atlyginimą už mokėjimo nurodymo atšaukimą, jeigu tai nustatyta bendrojoje sutartyje. 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, jei yra atitinkamas jo prašymas (pasibaigus 44 straipsnio 1 dalyje nurodytam terminui).

Remiantis ginčo byloje esančiais duomenimis, mokėjimo nurodymai įvykdyti ginčijamas mokėjimo operacijas buvo pateikti tiek prieš pareiškėjai kreipiantis į banką su prašymu šiuos mokėjimo nurodymus atšaukti, tiek ir prieš bankui informuojant pareiškėją apie tai, kad iš jos



su kortele susietos sąskaitos buvo įvykdytos ginčijamos mokėjimo operacijos, kurioms įvykdyti lėšos yra rezervuojamos – taigi, prašymas atšaukti mokėjimo nurodymus įvykdyti ginčijamas mokėjimo operacijas bankui buvo pateiktas po to, kai mokėjimo nurodymus jau buvo gavęs bankas, todėl Mokėjimų įstatyme nustatymas mokėjimo nurodymo atšaukimo terminas jau buvo praėjęs.

Pareiškėja kreipimesi į Lietuvos banką pažymi, kad 2021 m. gegužės 14 d. vykusio pokalbio su banko darbuotoja metu (tiek pirmojo, tiek vėlesnio) ji buvo informuota, kad jos sąskaitos banke yra blokuotos, o lėšos jose yra saugios, nors vėliau paaiškėjo, kad ši informacija yra klaidinga, nes pokalbio metu ginčijamų mokėjimo operacijų lėšos su kortele susietoje pareiškėjos banko sąskaitoje jau buvo rezervuotos, o 2021 m. gegužės 17 d. ir nurašytos trečiųjų asmenų naudai. Galima teigti, kad, pareiškėjos vertinimu, ši aplinkybė sukliudė bankui atšaukti lėšų rezervaciją ir ginčijamų mokėjimo operacijų sumos buvo nurašytos iš pareiškėjos sąskaitos banke. Atsižvelgdamas į šiuos pareiškėjos teiginius, bankas atsiliepime pažymi, kad dėl žmogiškosios klaidos nepastebėjusi pareiškėjos banko sąskaitoje lėšų, rezervuotų ginčijamoms mokėjimo operacijoms, kurios buvo inicijuotos panaudojant kortelę nuo 13 val. 11 min. iki 13 val. 41 min., įvykdyti, informavo pareiškėją, kad jos mokėjimo sąskaitoje paskutinė atlikta mokėjimo operacija yra lėšų pervedimas UAB „Tele2“. Vis dėlto analizuojamų aplinkybių kontekste ir atsižvelgiant į pirmiau nurodytas Mokėjimų įstatymo nuostatas, sutiktina su banko teiginiu, kad visos pareiškėjos ginčijamų mokėjimo operacijų sumos buvo rezervuotos mokėjimo operacijoms, kurios buvo inicijuotos dar iki pareiškėjos kreipimosi į banką ir atitinkamai – iki to momento, kai pareiškėja sužinojo (buvo informuota) apie neautorizuotas ginčijamas mokėjimo operacijas, todėl aplinkybė, kad 2021 m. gegužės 14 d. vykusio pokalbio metu banko darbuotoja neinformavo pareiškėjos apie jos sąskaitoje rezervuotas lėšas (t. y. suteikė klaidingą informaciją dėl lėšų su kortele susietoje sąskaitoje saugumo), neturi įtakos vertinimui, ar lėšos, rezervuotos iki pareiškėjos kreipimosi į banką, turėjo būti nurašytos iš pareiškėjos su kortele susietos sąskaitos. Kaip minėta, Mokėjimų įstatyme nustatytas mokėjimo nurodymo atšaukimo terminas pareiškėjos kreipimosi į banką metu jau buvo praėjęs, o kortelė ir interneto banko paskyra buvo blokuota tik po pareiškėjos kreipimosi į banką, todėl iki šio kreipimosi inicijuotoms mokėjimo operacijoms rezervuotų sumų nurašymo sustabdyti, nesant Mokėjimų įstatyme nustatyto pagrindo, bankas negalėjo.

Bankas taip pat paaiškino, kad, vadovaujantis mokėjimo kortelių organizacijos „MasterCard“ taisyklėmis, inicijavus ir priėmus vykdyti mokėjimo operacijas, atliktas mokėjimo kortele, lėšos su kortele susietoje sąskaitoje, siekiant užtikrinti vėlesnį lėšų nurašymą, pirmiausia yra rezervuojamos. Kai klientas suveda mokėjimo kortelės duomenis ir patvirtina mokėjimo operaciją prisijungimo priemone, mokėjimas jau būna įvykdytas ir lėšų rezervacijos panaikinimas. t. y. pinigų pervedimas prekybininkui, negali būti atšauktas. Šią banko poziciją patvirtina ir banko Taisyklių 13 skyriaus nuostatos, pagal kurias, davus sutikimą mokėjimo operacijai banko išduota mokėjimo kortele, bankas lėšas pirmiausia rezervuoja su mokėjimo kortele susietoje sąskaitoje. Remiantis 13 skyriaus nuostatomis, bankas atšaukia lėšų rezervavimą su mokėjimo kortele susietoje sąskaitoje, jei per 15 kalendorinių dienų nuo lėšų rezervavimo datos iš lėšų gavėjo bankas negauna patvirtinimo apie atsiskaitymą mokėjimo kortele. Vadinasi, bankas gali panaikinti (ir panaikina) lėšų rezervaciją tik tuo atveju, jei gaunamas gavėjo sutikimas dėl mokėjimo nurodymo atšaukimo arba lėšų gavėjo bankas nustatytais terminais nepateikia patvirtinimo apie atsiskaitymą mokėjimo kortele. Pažymėtina, kad tokios aplinkybės nagrinėjamo ginčo atveju nebuvo nustatytos, taigi, nebuvo nustatytos ir sąlygos, kada pagal Taisyklių sąlygas mokėjimo operacijoms, patvirtintoms šalių sutartu būdu, įvykdyti pritaikytą lėšų rezervaciją bankas gali panaikinti. Pažymėtina, kad tokia aplinkybė nagrinėjamo ginčo atveju nebuvo nustatyta, todėl nebuvo nustatytos ir sąlygos, kada pagal Taisyklių sąlygas mokėjimo operacijoms, patvirtintoms šalių sutartu būdu, nustatyta rezervacija yra naikintina.

#### *Dėl ginčijamų mokėjimo operacijų lėšų gražinimo*

Pažymėtina, kad pareiškėjos reikalavimas atlyginti jos nuostolius, galėjusius, pareiškėjos teigimu, atsirasti dėl banko veiksmų, netinkamai vykdant jos prašymą atšaukti ginčijamas mokėjimo operacijas, savo esme yra reikalavimas taikyti civilinę atsakomybę banko atžvilgiu. Pagal civilinės atsakomybės sampratą, civilinė atsakomybė – tai turtinė prievolė, kurios viena šalis turi teisę reikalauti atlyginti nuostolius (žalą) ar sumokėti netesybas, o kita šalis privalo atlyginti padarytus nuostolius (žalą) ar sumokėti netesybas (Lietuvos Respublikos civilinio kodekso (CK) 6.245 straipsnio 1 dalis). Vadovaujantis CK 6.246 straipsnio 1 dalimi,



civilinė atsakomybė atsiranda neįvykdžius įstatymuose ar sutartyje nustatytos pareigos (neteisėtas neveikimas) arba atlikus veiksmus, kuriuos įstatymai ar sutartis draudžia atlikti (neteisėtas veikimas), arba pažeidus bendro pobūdžio pareigą elgtis atidžiai ir rūpestingai. Taigi, civilinė atsakomybė atsiranda esant asmens, įpareigoto atlikti atitinkamus veiksmus ar nuo jų susilaikyti, neteisėtiems veiksams ar neveikimui, taip pat kaltei dėl šių neteisėtų veiksmų padarymo ar neveikimo, žalai ir priežastiniam ryšiui tarp veiksmų ar neveikimo ir atsiradusios žalos (CK 6.246–6.249 straipsniai)<sup>14</sup>. Be to, CK 6.256 straipsnio 4 dalyje nustatyta, kad tuo atveju, kai sutartinės prievolės neįvykdo ar netinkamai ją įvykdo įmonė (verslininkas), tai ji atsako visais atvejais, jei neįrodo, kad prievolės neįvykdė ar netinkamai ją įvykdė dėl nenugalimos jėgos, jeigu įstatymuose ar sutartyje nenumatyta ko kita. Kasacinis teismas savo praktikoje ne kartą yra pažymėjęs, kad sutartinei civilinei atsakomybei žalos (įskaitant negautas pajamas) atlyginimo forma (CK 6.245 straipsnio 3 dalis, 6.256 straipsnis) taikyti nepakanka sutarties neįvykdymo (pažeidimo) fakto, sutartinei civilinei atsakomybei taikyti yra būtinas šių sąlygų visetas – bent vienos sąlygos nebuvimas eliminuoja civilinės atsakomybės taikymo galimybę<sup>15</sup>. Taigi, nagrinėjamu atveju civilinė atsakomybė banko atžvilgiu bendraisiais CK nustatytais pagrindais būtų taikoma tik nustačius visų trijų civilinės atsakomybės sąlygų – neteisėtų banko veiksmų, pareiškėjos nuostolių (žalos) dėl ginčijamų mokėjimo operacijų ir priežastinio ryšio tarp neteisėtų banko veiksmų ir pareiškėjos nuostolių – visumą.

Ginčo nagrinėjimo metu nustatyta ir šalių neginčijama aplinkybė, kad pareiškėja dėl neautorizuotų ginčijamų mokėjimo operacijų patyrė nuostolių.

Vertinant, ar nustatytos prielaidos konstatuoti banko neteisėtus veiksmus, kaip būtinąją civilinės atsakomybės taikymo sąlygą, reikia vadovautis ginčo byloje esančiais duomenimis ir ginčo nagrinėjimo metu nustatytais aplinkybėmis (jų visuma). Kaip jau buvo konstatuota pirmiau, banko veiksmai, įvykdant pareiškėjos ginčijamas mokėjimo operacijas, vertintini kaip teisėti ir pagrįsti – atitinkantys Mokėjimų įstatymo reikalavimus ir šalių susitarimo sąlygas. Vertinant, ar bankas tinkamai įvykdė pareiškėjos prašymą atšaukti mokėjimo nurodymus įvykdyti ginčijamas mokėjimo operacijas, turėtų būti analizuojamos ginčo nagrinėjimo metu nustatytos aplinkybės.

2021 m. gegužės 14 d. 14 val. 50 min. pareiškėjai kreipusis telefonu į banką, banko darbuotoja pokalbio metu įvertino situaciją pagal pareiškėjos nurodytas aplinkybes ir, atsižvelgusi taip pat ir į pareiškėjos prašymą, užblokavo pareiškėjos kortelę (15 val. 9 min.), interneto banko paskyrą (14 val. 51 min.), atšaukė pareiškėjos vardu pateiktą vartojimo kredito paraišką 3 000 Eur sumai (15 val. 36 min.). To paties telefoninio pokalbio metu banko darbuotoja patikrino pareiškėjos vardu sudarytas „Smart-ID“ tapatybės patvirtinimo priemonės sutartis ir informavo pareiškėją, kad 2021 m. gegužės 14 d. pareiškėjos vardu buvo sukurta nauja prisijungimo priemonė – programėlė „Smart-ID“ kitame telefono įrenginyje, todėl patarė pareiškėjai nedelsiant kreiptis į „Smart-ID“ tapatybės patvirtinimo priemonės išdavėją „SK ID Solutions AS“ dėl „Smart-ID“ paskyros blokavimo ir panaikinimo, o dėl galimo sukčiavimo, duomenų atskleidimo kitiems asmenims – į policiją. Aptartos aplinkybės leidžia teigti, kad bankas tinkamai ir laiku įvykdė pareiškėjos prašymą užblokuoti banko jai išduotas mokėjimo priemones, taip pat informavo apie būtinybę kreiptis į „Smart-ID“ tapatybės patvirtinimo priemonę išdavusią įmonę dėl šios tapatybės priemonės blokavimo (informavimo apie sukčiavimo atvejį) ir į policiją dėl galėjusios įvykti nusikalstamos veikos ištyrimo.

Vertinant, ar bankas tinkamai veikė vykdydamas pareiškėjos prašymą atšaukti mokėjimo nurodymus įvykdyti ginčijamas mokėjimo operacijas ir gražinti šių operacijų lėšas pareiškėjai, atsižvelgtina į toliau dėstomas aplinkybes. Ginčijamų mokėjimo operacijų įvykdymo dieną vykusio pokalbio metu banko darbuotoja dėl žmogiškosios klaidos nepastebėjusi pareiškėjos su kortele susietoje sąskaitoje lėšų, rezervuotų mokėjimo operacijoms, kurios buvo inicijuotos panaudojant kortelę tą dieną nuo 13 val. 11 min. iki 13 val. 41 min., įvykdyti, informavo pareiškėją, kad jos mokėjimo sąskaitoje paskutinė atlikta mokėjimo operacija yra lėšų pervedimas UAB „Tele2“, taip pat nurodė, kad pareiškėjos sąskaita, susieta su kortele, tiek ir pati kortelė yra blokuotos, todėl pareiškėjos lėšos yra saugios. Bankas atsiliepime Lietuvos bankui pripažįsta, kad ginčijamų mokėjimo operacijų įvykdymo dieną vykusių pokalbių metu banko darbuotoja klaidingai informavo pareiškėją, kad jos sąskaitoje paskutinė atlikta mokėjimo operacija yra lėšų pervedimas UAB „Tele2“, taip pat nurodė, kad pareiškėjos lėšos yra saugios, nors tokia informacija, kaip minėta, buvo klaidinga. Vis dėlto konstatuota

<sup>14</sup> Lietuvos Aukščiausiojo Teismo Civilinių bylų skyriaus teisėjų kolegijos 2002 m. balandžio 15 d. nutartis, priimta civilinėje byloje UAB „Vasario koncernas“ v. Teisingumo ministerija, bylos Nr. 3K-3-600/2002.

<sup>15</sup> Lietuvos Aukščiausiojo Teismo 2018 m. balandžio 13 d. nutartis civilinėje byloje Nr. 3K-3-144-915/2018, 31 punktą.

aplinkybė, kad banko darbuotoja suteikė klaidingą informaciją dėl lėšų su kortele susietoje sąskaitoje saugumo, savaime nesuponuoja išvados, jog priešingi banko veiksmai – tikslios ir teisingos informacijos apie lėšų rezervacijas su kortele susietoje sąskaitoje suteikimas, būtų lėmę kitokį banko, kaip mokėjimo paslaugų teikėjo, Mokėjimų įstatyme įtvirtintų pareigų, susijusių su mokėjimo nurodymų įvykdymu ir (ar) jų atšaukimu, vertinimą. Taigi, dėl šio aspekto sutiktina su banko atsiliepime nurodyta aplinkybe, kad visos pareiškėjos ginčijamų mokėjimo operacijų sumos buvo rezervuotos mokėjimo operacijoms, kurios buvo inicijuotos ir patvirtintos dar iki pareiškėjos kreipimosi į banką, ir atitinkamai – iki to momento, kai pareiškėja sužinojo apie neautorizuotas ginčijamas mokėjimo operacijas. Taigi, net ir tuo atveju, jei 2021 m. gegužės 14 d. vykusio pokalbio metu banko darbuotoja būtų teisingai informavusi pareiškėją apie jos sąskaitoje rezervuotas lėšas, tai nebūtų turėję įtakos lėšų, rezervuotų iki pareiškėjos kreipimosi į banką, nurašymui iš pareiškėjos su kortele susietos sąskaitos. Kaip buvo konstatuota pirmiau, prašymas atšaukti mokėjimo nurodymus įvykdyti ginčijamas mokėjimo operacijas bankui buvo pateiktas po to, kai mokėjimo nurodymus jau buvo gavęs bankas, todėl Mokėjimų įstatyme nustatytas mokėjimo nurodymo atšaukimo terminas jau buvo praėjęs<sup>16</sup>.

Pareiškėja kreipimesi taip pat teigia, kad bankas neinformavo jos apie galimybę kreiptis į tarpininko įmonę dėl ginčijamų mokėjimo operacijų atšaukimo. Apie tokią galimybę pareiškėja teigia sužinojusi tik iš policijos pareigūno, ir tai, pareiškėjos teigimu, padėjo jai susigrąžinti paskutinės (aštuntosios) ginčijamos mokėjimo operacijos sumą. Iš pareiškėjos kreipimesi dėstomų teiginių galima numanyti, kad, pareiškėjos vertinimu, jei bankas laiku, t. y. iškart pareiškėjai paskambinus į banką ir paprašius patikrinti jos sąskaitą, būtų informavęs pareiškėją apie jos sąskaitoje rezervuotas lėšas ginčijamoms mokėjimo operacijoms įvykdyti, taip pat būtų pataręs kreiptis į *TransferGo* dėl mokėjimo nurodymų įvykdyti ginčijamas mokėjimo operacijas atšaukimo bei tokių operacijų lėšų gražinimo, pareiškėjai būtų pavykę atgauti ir kitų septynių ginčijamų mokėjimo operacijų lėšas.

Pažymėtina, kad nors finansų rinkos dalyviai, tarp jų ir bankas, teikdami finansines paslaugas, turi veikti profesionaliai ir skaidriai, o klientams jų teikiama informacija apie paslaugas turi būti aiški, išsami ir teisinga, tačiau teisės aktai mokėjimo paslaugų teikėjams (taigi, ir bankui) nenustato pareigos informuoti savo klientų, ginčijančių tam tikrą mokėjimo operaciją, apie galimybę kreiptis į lėšų pervedimo tarpininką dėl šių lėšų susigrąžinimo. Vis dėlto neabejotina, kad bankui, kaip kiekvienam kitam mokėjimo paslaugų teikėjui, tenkanti bendroji rūpestingumo pareiga lemia tai, kad bankas turi veikti, siekdamas padėti klientui, mokėjimo paslaugų vartotojui, atgauti jo lėšas dėl neautorizuotų ir (ar) ginčijamų mokėjimo operacijų, ypač sukčiavimų elektroninėje erdvėje atvejais. Be to, bankų veiklą reguliuojančio Lietuvos Respublikos bankų įstatymo tikslas – „reglamentuoti bankų ir užsienio bankų, veikiančių Lietuvos Respublikoje, taip pat jų padalinių steigimo, licencijavimo, veiklos, pabaigos ir pertvarkymo bei priežiūros tvarką, kad bankų sistema būtų stabili, patikima, efektyvi ir saugi“<sup>17</sup>. Stabilumo, patikimumo, efektyvumo ir saugumo principai formuoja aukštus banko veiklos, kaip atskiros profesinės veiklos rūšies, apdairumo ir rūpestingumo standartus. Banko, kaip specializuotos finansų įstaigos, pareiga profesinėje veikloje elgtis apdairiai ir rūpestingai apima bendrąją banko pareigą garantuoti šios veiklos patikimumą, efektyvumą ir saugumą<sup>18</sup>, tačiau, taikant bankui aukštesnius patikimumo ir rūpestingumo standartus, turi būti nustatyta, kad banko išduodamos personalizuotos sąskaitos saugumo priemonės nepakankamai apsaugo vartotojo sąskaitą, jei įstatyme nenustatyta kitaip<sup>19</sup>. Bankui, kaip profesionaliam verslininkui ir savo srities specialistui, yra keliami aukštesni profesionalumo, atidumo ir rūpestingumo standartai, todėl, turėdamas specifinių finansinių paslaugų teikimo srities žinių, bankas turėtų dėti reikiamas ir protingai įmanomas pastangas (įskaitant ir teisingos, išsamios ir visapusiškos informacijos apie ginčijamų mokėjimo operacijų lėšų susigrąžinimą) tam, kad klientai, kurie, net ir būdami neatsargūs ar labai neatsargūs, galėjo prarasti lėšas dėl neautorizuotų mokėjimo operacijų, turėtų visas galimybes šias lėšas atgauti. Tai, kad verslininkui, kartu ir bankui, kaip ir bet kuriam kitam savo srities profesionalui, teikiančiam paslaugas, teisės aktuose nustatytas aukštesnis profesionalo teisėto elgesio standartas, taigi, jam taikomi aukštesni profesionalumo, atidumo ir rūpestingumo standartai, savo praktikoje ne kartą yra pabrėžęs ir kasacinis

<sup>16</sup> Mokėjimų įstatymo 44 straipsnio 1 dalis.

<sup>17</sup> Bankų įstatymo 1 straipsnio 1 dalis.

<sup>18</sup> Lietuvos Aukščiausiojo Teismo 2002 m. vasario 20 d. nutartis civilinėje byloje Nr. 3K-3-390/2002.

<sup>19</sup> Lietuvos Aukščiausiojo Teismo 2017 m. gegužės 9 d. nutartis civilinėje byloje Nr. 3K-3-222-219/2017.

teismas<sup>20</sup>. Vertindamas civilinės atsakomybės taikymo klausimus, kasacinis teismas taip pat yra pažymėjęs, kad sutarčių teisėje ypač svarbus vaidmuo tenka sąžiningumo principui. Viena iš svarbiausių šio principo išraiškos formų yra šalių tarpusavio bendradarbiavimo pareiga sutartinių santykių metu. Sutarties šalių bendradarbiavimo procesas turi vykti sąžiningumo ir geros valios sąlygomis. Tai reiškia, kad sutarties šalies elgesys negali būti priešingas tiems lūkesčiams, kuriuos ji savo veiksmais, atliktais vykdant sutarties sąlygas, suformavo kitai sutarties šaliai<sup>21</sup>.

Ginčo nagrinėjimo metu nustatytos ir pirmiau aptartos aplinkybės, t. y. kad banko darbuotoja suteikė pareiškėjai klaidingą informaciją apie jos lėšų sąskaitoje saugumą, neatkreipė pareiškėjos dėmesio į egzistuojančias visas galimybes bandyti susigražinti ginčijamų mokėjimo operacijų lėšas (pvz., kreiptis į *TransferGo*), nesudaro pagrindo teigti, kad banko veiksmai visiškai atitiko jam, kaip profesionaliam verslininkui ir savo srities specialistui, keliamus aukštus profesionalumo, atidumo ir rūpestingumo standartus, taigi, nesudaro pagrindo teigti, kad bankas būtų tinkamai įvykdęs jam keliamą bendro pobūdžio pareigą elgtis itin atidžiai ir rūpestingai, dėti visas pastangas bendradarbiaujant su pareiškėja.

Kita vertus, vertinant priežastinį ryšį tarp banko veiksmų (neveikimo) ir pareiškėjos nuostolių, svarbu nustatyti, ar banko veiksmai (neveikimas) buvo pareiškėjos nuostolių atsiradimo priežastis. Priežastinio ryšio samprata pateikiama CK 6.247 straipsnyje: atlyginami tik tie nuostoliai, kurie susiję su veiksmais (veikimu, neveikimu), nulėmusiais skolininko civilinę atsakomybę tokiu būdu, kad nuostoliai pagal jų ir civilinės atsakomybės prigimtį gali būti laikomi skolininko veiksmų (veikimo, neveikimo) rezultatu. Kasacinio teismo praktikoje nuosekliai pažymima, kad CK 6.247 straipsnyje įtvirtinta lankstaus priežastinio ryšio samprata. Priežastinio ryšio lankstus taikymas atitinka civilinės atsakomybės tikslą kompensuoti padarytus nuostolius, kurių atsiradimas yra susijęs su veikimu ar neveikimu, dėl kurio šie nuostoliai atsirado<sup>22</sup>. Vis dėlto ginčo byloje turimi duomenys ir įrodymai teigti, kad pareiškėjos nuostoliai dėl ginčijamų mokėjimo operacijų šiuo atveju kyla iš tam tikrų banko veiksmų ar neveikimo, nesuteikia pakankamo pagrindo: ginčo nagrinėjimo metu nustatytais duomenimis, pareiškėjos nuostoliai kilo dėl neteisėtos veikos (sukčiavimo elektroninėje erdvėje), įvykdytos trečiųjų asmenų, kurie neteisėtais veiksmais sukūrė naują tapatybės patvirtinimo priemonės „Smart-ID“ paskyrą savo valdomame mobilijame įrenginyje, ir be pareiškėjos žinios bei valinių veiksmų inicijavo ir patvirtino ginčijamas mokėjimo operacijas. Vadinasi, jei nebūtų buvę trečiųjų asmenų neteisėtų veiksmų, kurie buvo įvykdyti dar iki pareiškėjos kreipimosi į banką, pareiškėjos nuostoliai – iš sąskaitos nurašytos lėšos dėl ginčijamų mokėjimo operacijų, nebūtų atsiradę.

Vertinamų aplinkybių kontekste atkreiptinas dėmesys ir į tai, kad ginčo byloje nėra jokių duomenų, kurie leistų pagrįstai teigti, kad kuri nors iš septynių pareiškėjos ginčijamų mokėjimo operacijų sumų būtų buvusi pareiškėjai gražinta, jei ji būtų anksčiau kreipusis į *TransferGo*. Priešingai, ginčo nagrinėjimo metu bankas pateikė papildomų duomenų, susijusių su pareiškėjos ginčijamų mokėjimo operacijų lėšų nurašymu iš *TransferGo* esančios sąskaitos: bankas, kreipėsi į minėtą mokėjimo paslaugų teikėją, prašydamas patikslinti lėšų pervedimo laikus iš *TransferGo* esančios sąskaitos, į kurią buvo įskaitytos lėšos, gautos iš pareiškėjos. *TransferGo* pateikė bankui atsakymą, kad lėšos iš sąskaitos, esančios *TransferGo*, buvo nurašytos 2021 m. gegužės 14 d. nuo 13 val. 11 min. iki 13 val. 38 min. Lietuvos laiku, t. y. iki to laiko, kai pareiškėja dėl ginčijamų mokėjimo operacijų kreipėsi į banką (14 val. 50 min.).

Bankas pažymi, kad lėšos iš sąskaitos *TransferGo* buvo pervestos į galutinę lėšų gavėjo sąskaitą beveik dvi valandos iki to laiko, kai pareiškėja pirmą kartą kreipėsi į dėl ginčijamų mokėjimo operacijų, todėl šių operacijų lėšų gražinimas tuo laiku, kai pareiškėja paskambino bankui dėl ginčijamų mokėjimo operacijų, jau buvo techniškai neįmanomas – lėšų gavėjo sąskaitoje neliko. Kartu su papildomais paaiškinimais bankas taip pat pateikė banko iš *TransferGo* gautą atsakymą, kuriame pateikiami paaiškinimai dėl pareiškėjos ginčijamų mokėjimo operacijų įvykdymo aplinkybių. Minėtame *TransferGo* atsakyme bankui nurodyta, kad aštuntoji pareiškėjos ginčijama mokėjimo operacija buvo sustabdyta, o jos sustabdymo ir lėšų gražinimo priežastis – dienos limito viršijimas, kurį viršijus *TransferGo* paprašė savo kliento

<sup>20</sup> Pavyzdžiui, Lietuvos Aukščiausiojo Teismo 2008 m. vasario 28 d. nutartis civilinėje byloje Nr. 3K-3-112/2008; 2010 m. kovo 1 d. nutartis civilinėje byloje Nr. 3K-3-69/2010; 2018 m. spalio 12 d. nutartis civilinėje byloje Nr. e3K-3-60-969/2018.

<sup>21</sup> Lietuvos Aukščiausiojo Teismo 2014 m. vasario 14 d. nutartis civilinėje byloje Nr. 3K-3-29/2014; 2021 m. kovo 24 d. nutartis civilinėje byloje Nr. e3K-3-44-313/2021.

<sup>22</sup> Lietuvos Aukščiausiojo Teismo 2013 m. spalio 22 d. nutartis civilinėje byloje Nr. 3K-3-531/2013.

pateikti lėšų kilmę patvirtinančius dokumentus ir jų negavusi, negalėdama nustatyti lėšų kilmės, būtent dėl šios priežasties *TransferGo* savo iniciatyva grąžino 1 185 Eur mokėjimo operacijos lėšas pareiškėjai. Taigi, ginčo byloje nėra jokių duomenų ir juos pagrindžiančių įrodymų, kad banko veiksmai, suteikiant klaidingą informaciją pareiškėjai apie lėšų jos sąskaitoje saugumą ir neinformavimas apie įvykusias neautorizuotas mokėjimo operacijas, taip pat informacijos apie galimybę kreiptis į *TransferGo* nesuteikimas, būtų užkirte kelią pareiškėjai susigražinti dėl neautorizuotų mokėjimo operacijų prarastas lėšas ar bent jų dalį (taigi, sumažinti žalą) iš *TransferGo* ir tai būtų buvę šių pareiškėjos nuostolių atsiradimo priežastimi. Kitaip tariant, aplinkybė, kad banko veiksmai neatitiko bankui, kaip profesionaliam verslininkui ir savo srities specialistui, keliamų standartų ir bendroji rūpestingumo pareiga iš banko pusės nebuvo įvykdyta taip, kaip būtų galima tikėtis iš banko, kaip ir bet kurio kito mokėjimo paslaugų teikėjo, tokioje situacijoje, kai nėra jokių patikimų priešingą poziciją pagrindžiančių įrodymų, nereiškia, kad pareiškėja būtų išvengusi nuostolių. Kaip buvo minėta pirmiau, ginčo byloje esantys duomenys (banko ginčo nagrinėjimo metu papildomai pateikta informacija) leidžia teigti priešingai, t. y. pareiškėja būtų patyrusi nuostolių dėl ginčijamų mokėjimų operacijų, net ir tuo atveju, jei bankas būtų elgęsis apdairiai, rūpestingai ir profesionaliai, kaip ir kiek buvo būtina šioje situacijoje, taigi, laiku ir tinkamai būtų suteikęs išsamią ir teisingą informaciją pareiškėjai dėl ginčijamų mokėjimo operacijų.

Pažymėtina, kad priežastinis ryšys yra būtinoji civilinės atsakomybės sąlyga – nenustačius priežastinio ryšio tarp neteisėtų veiksmų ir žalos, nėra pagrindo civilinei atsakomybei kilti<sup>23</sup>. Kaip konstatuota pirmiau, civilinei atsakomybei taikyti būtina nustatyti civilinės atsakomybės sąlygų visetą: tai reiškia, kad, neįrodžius bent vienos iš nurodytų atsakomybės sąlygų, žalos atlyginimas negalimas, nes žalai atlyginti nėra teisinio pagrindo<sup>24</sup>. Taigi, nagrinėjamu atveju nenustačius visų banko civilinės atsakomybės taikymo sąlygų, pripažinti pareiškėjos teisę reikalauti iš banko nuostolių atlyginimo nėra teisinio pagrindo.

Vadovaujantis nustatytomis aplinkybėmis ir atsižvelgiant į tai, kad bankas, kai nėra Mokėjimų įstatyme ir Taisyklėse nustatytų sąlygų, negalėjo atšaukti mokėjimo nurodymų įvykdyti ginčijamas mokėjimo operacijas ir grąžinti pareiškėjai šių operacijų sumų, praėjus mokėjimo nurodymo atšaukimo terminui, taip pat atsižvelgiant į tai, kad nebuvo nustatytos visos būtinosios banko civilinės atsakomybės taikymo sąlygos, darytina išvada, kad tenkinti pareiškėjos reikalavimo ir rekomenduoti bankui kompensuoti pareiškėjai jos nuostolius dėl įvykdytų ginčijamų mokėjimo operacijų nėra teisinio pagrindo, todėl pareiškėjos reikalavimas atmestinas.

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. Vartotojas ir finansų rinkos dalyvis turi teisę dėl ginčo sprendimo kreiptis į teismą arba kitą ginčų nagrinėjimo instituciją įstatymų nustatyta tvarka. Kreipimasis į teismą po Lietuvos banko sprendimo dėl ginčo esmės priėmimo nelaikomas šio sprendimo apskundimu.

Direktorius

Arūnas Raišutis

<sup>23</sup> Lietuvos Aukščiausiojo Teismo 2011 m. gruodžio 7 d. nutartis civilinėje byloje Nr. 3K-3-478/2011; 2012 m. kovo 15 d. nutartis civilinėje byloje Nr. 3K-3-94/2012.

<sup>24</sup> Lietuvos Aukščiausiojo Teismo 2009 m. vasario 4 d. nutartis civilinėje byloje Nr. 3K-3-5/2009; 2010 m. gegužės 24 d. nutartis civilinėje byloje Nr. 3K-3-219/2010; 2013 m. gruodžio 4 d. nutartis civilinėje byloje Nr. 3K-3-634/2013; kt.