LIETUVOS BANKO TEISĖS IR LICENCIJAVIMO DEPARTAMENTO DIREKTORIUS

SPRENDIMAS DĖL X.X. IR „PAYSERA LT", UAB, GINČO NAGRINĖJIMO

2022-03-24 Nr. 429-89
Vilnius

Lietuvos bankas gavo X.X. (toliau – pareiškėja) kreipimąsi, kuriuo prašoma išnagrinėti tarp pareiškėjos ir „Paysera LT", UAB, (toliau – bendrovė) kilusį ginčą.

N u s t a t y t a:

2021 m. lapkričio 5 d. prisijungus prie pareiškėjos paskyros bendrovėje iš pareiškėjos sąskaitos buvo atliktos trys mokėjimo operacijos gavėjui Hyppolite'ui Abel'iui Nade (Hyppolite Abel Nade) (toliau – gavėjas) į jo sąskaitą bendrovėje: 18:57:43 val. 1 000 Eur; 19:05:39 val. 1 000 Eur ir 19:07:04 val. 1 000 Eur (toliau – mokėjimo operacijos).

Pareiškėja 2021 m. lapkričio 5 d. 19:02:50 val. telefonu kreipėsi į bendrovę ir pranešė apie galimai trečiųjų asmenų neteisėtu būdu iš pareiškėjos pasisavintus prisijungimo prie jos paskyros duomenis ir įvykdytą pareiškėjos neautorizuotą mokėjimo operaciją. Pareiškėjai kalbantis su bendrovės darbuotoju telefonu, buvo įvykdytos dar dvi mokėjimo operacijos, kurioms pareiškėja teigė nedavusi sutikimo. Bendrovė nustačiusi pareiškėjos tapatybę 19:10:32 val. apribojo naudojimąsi pareiškėjos sąskaita, o 19:17:38 val. apribojo gavėjo sąskaitą. 2021 m. lapkričio 9 d. bendrovė į pareiškėjos sąskaitą grąžino 2 600 Eur, tokią sumą bendrovei pavyko sulaikyti gavėjo sąskaitoje. Vis dėlto likusios 400 Eur sumos bendrovė pareiškėjai negalėjo grąžinti, nes minėta suma jau buvo išimta iš lėšų gavėjo sąskaitos.

Bendrovei nesutikus pareiškėjai grąžinti likusios 400 Eur sumos, pareiškėja kreipėsi į Lietuvos banką dėl vartojimo ginčo nagrinėjimo. Pareiškėja Lietuvos bankui paaiškino, kad „2021 m. lapkričio 5 d. apie 5 min. prieš 19 val. aš prisijungiau prie mano *Payseros* sąskaitos ir iš pradžių dar savo mobiliame telefone, per kurį aš prisijungimą aktyvavau, pamačiau, kad kažkas padarė pavedimą 2 000 Eur į man nežinomo žmogaus sąskaitą. Visgi prie mano kompiuterio prisijungus aš to pavedimo nebemačiau ir maniau, kad tai sistemos klaida. Praktiškai tik minutei praėjus 18:57 val. iš mano *Paysera* sąskaitos buvo pervesta pirma suma 1 000 Eur man nepažįstamam žmogui *Hyppolite Abel Nade*". Pareiškėja teigė, kad iš karto, kai tai pastebo, telefonu kreipėsi į bendrovę ir pranešė apie iš pareiškėjos sąskaitos atliktą pareiškėjos neautorizuotą mokėjimo operaciją, tačiau, kol bendrovės darbuotojas kalbėjosi su pareiškėja, iš pareiškėjos sąskaitos bendrovėje buvo padaryti dar du mokėjimo pavedimai, kuriems pareiškėja teigė nedavusi sutikimo.

Pareiškėja teigė iš bendrovės gavusi atsakymą, kad pareiškėja dėl savo didelio neatsargumo prisijungė prie suklastoto bendrovės puslapio *www.paeyserra.com* ir jame suvedė savo prisijungimo duomenis, įskaitant SMS žinute gautą vienkartinį saugos kodą, dėl to tretieji asmenys nusavino pareiškėjos prisijungimo prie paskyros duomenis ir be pareiškėjos žinios ir sutikimo inicijavo mokėjimo operacijas. Pareiškėja paaiškino, kad, jungdamasi prie bendrovės paskyros *www.google.de*, paieškos sistemoje suvedė bendrovės pavadinimą ir paspaudė patį pirmą paieškos sistemos pateiktą pasirinkimą. Vėliau paaiškėjo, kad tai buvo trečiųjų asmenų suklastota bendrovės svetainė su suklastotu bendrovės svetainės adresu *www.paeyserra.com*. Pareiškėja teigė nepastebėjusi, kad tai suklastotas bendrovės interneto svetainės adresas, o pati suklastota bendrovės svetainė atrodė kaip tikra, todėl pareiškėjai nekilo jokių įtarimų, kad tai gali būti netikra bendrovės interneto svetainė. Pareiškėja patikino, kad tokio pobūdžio trečiųjų asmenų neteisėtų veiksmų ataka prieš bendrovės klientus buvo ne pirma, todėl, pareiškėjos nuomone, bendrovė turėjo ir galėjo užtikrinti, kad *Google* paieškos sistemoje pirmu pasirinkimu neatsirastų sukčių suklastota nuoroda į bendrovės svetainę, tačiau bendrovė, net ir žinodama apie tokio pobūdžio atakas, nesiėmė jokių veiksmų, kad užkirstų kelią sukčių

atakoms.

Papildomai pareiškėja atkreipė dėmesį, kad bendrovė mokėjimo operacijai patvirtinti neprašo įvesti PIN kodo slaptažodžio, todėl, pareiškėjos teigimu, bendrovės sistemos nėra pakankamai saugios. Pareiškėjos teigimu, jeigu bendrovėje veiktų *Two factor autentification* sistema, t. y. į pareiškėjos mobiluįį telefoną būtų atsiųsta SMS žinutė apie inicijuojamą mokėjimo operaciją ir prašymas tą konkrečią mokėjimo operaciją patvirtinti PIN kodo slaptažodžiu, pareiškėja būtų išvengusi lėšų praradimo. Taip pat pareiškėja paaiškino, kad bendrovė nesiunčia žinučių apie įvykdytas mokėjimo operacijas, todėl, jeigu pareiškėja atsitiktinai nebūtų prisijungusi prie savo paskyros, ji nebūtų pastebėjusi iš jos sąskaitos įvykdytų mokėjimo operacijų.

Pareiškėja taip pat teigė nesutinkanti su bendrovės argumentais, kad neva ji prisijungdama prie sukčių suklastotos bendrovės paskyros buvusi labai neatsargi, nes jungtis prie bendrovės paskyros iš skirtingų valstybių ir skirtingų įrenginių jai buvo įprastas veiksmas. Pareiškėja ne vieną kartą SMS žinute buvo gavusi vienkartinį saugos kodą, kurį ir suvesdavo tam, kad patvirtintų prisijungimą prie savo paskyros bendrovėje iš kitos valstybės ir įrenginio. Paminėtina, kad, ginčo byloje turimais duomenimis, pareiškėja nuolat gyvena Vokietijoje ir prie savo paskyros bendrovėje neretai jungiasi iš skirtingų valstybių bei įrenginių.

Papildomai pareiškėja nurodė savo veiksmų seką, po kurios pastebėjo, kad iš jos sąskaitos bendrovėje be pareiškėjos žinios ir sutikimo buvo įvykdytos mokėjimo operacijos. Pareiškėja paaiškino, kad „mano prisijungimas buvo vykdomas tokia seka: 1. Aš paspaudžiau reklaminę nuorodą *Google* sistemoje į netikrą bendrovės puslapį, bet joje įvedžiau tik savo emailą ir slaptažodis jau buvo užsaugotas mano kompiuteryje. Kadangi tai dar buvo senas slaptažodis ir aš jo negalėjau pakeisti, nes man to mano kompiuteris neleido, aš jungiausi pasirinkusi kompiuterio programėlę. Be to man rodė, kad prisijungiama iš kito įrenginio, kas yra normalu, nes aš buvau išvažiavus į Ameriką ir žinoma buvo mano kitas UR, taigi gauti tą SMS su kodu buvo įprastas procesas, kurį aš esu mačiusi *Payseros* aptarnavime anksčiau. Todėl aš negalėjau pastebėti, kad suklastotas bendrovės svetainės adresas skiriasi nuo to, kuris yra bendrovės – www.bank.paysera.com, nes žinutė to nenurodo ir viskas vyko taip, kaip aš įprastai prisijungiu prie *Payseros* banko būdama kitoje šalyje.“ Papildomai pareiškėja telefonu Lietuvos bankui detalizavo, kad, *Google* paieškos sistemoje paspaudusi sukčių suklastotą nuorodą į bendrovės interneto puslapį, suvedė ne tik savo prisijungimo prie paskyros duomenis, bet ir SMS žinute gautą vienkartinį saugos kodą.

Pareiškėja teigė, kad, jai kreipusis į bendrovę telefonu ir pranešus apie galimai prarastus personalizuotus saugos duomenis bei iš jos sąskaitos įvykdytą neautorizuotą mokėjimo operaciją, bendrovė nesiėmė visų būtinų veiksmų ir laiku neapribojo naudojimosi jos sąskaita, dėl to tretieji asmenys jai besikalbant su bendrovės darbuotoju telefonu įvykdė dar dvi pareiškėjos neautorizuotas mokėjimo operacijas.

Pareiškėja teigė, kad nors bendrovė jai grąžino dalį pinigų sumos – 2 600 Eur, tačiau, pareiškėjos teigimu, nėra aišku, kodėl bendrovė laiku nesustabdė mokėjimo operacijų, nors ir gavėjo sąskaita buvo toje pačioje bendrovėje. Pareiškėja prašė bendrovės grąžinti 400 Eur.

Bendrovė Lietuvos bankui pateiktame atsiliepime paaiškino, kad pripažįsta, kad pareiškėja galėjo tapti trečiųjų asmenų neteisėtų veiksmų auka, dėl to tretieji asmenys galėjo nusavinti pareiškėjos prisijungimo prie paskyros duomenis ir iš pareiškėjos sąskaitos be pareiškėjos žinios ir sutikimo įvykdyti pareiškėjos neautorizuotas mokėjimo operacijas. Kaip bendrovė paaiškino savo atsiliepime, bendrovė identifikavo, kad pareiškėja dėl didelio savo neatsargumo pasidalijo savo prisijungimo duomenimis su galimai nusikalstamą veiką organizavusiais asmenimis ir taip prarado pinigines lėšas.

Bendrovės teigimu, pareiškėja dėl savo didelio neatsargumo neišsaugojo savo prisijungimo prie paskyros duomenų, nes:

1. Prieš atlikdama mokėjimo operacijas 18:41 val. (Lietuvos laiku) *www.google.de* naršyklės paieškos laukelyje pareiškėja suvedė *Paysera* raktažodį, o pasirodžius paieškos rezultatams pasirinko reklaminę nuorodą į suklastotą puslapį *www.paeyserra.com.*

2. Šiame suklastotame interneto puslapyje pareiškėja suvedė savo prisijungimo prie *Paysera* sistemos duomenis ir taip savo prisijungimo duomenimis pasidalijo su trečiaisiais asmenimis, šie tuo pačiu metu panaudojo iš pareiškėjos gautus jos prisijungimo duomenis jungdamiesi prie tikrosios pareiškėjos sąskaitos *Paysera* programėlėje savo įrenginyje iš IP adreso Nr. 84.247.51.236 Prancūzijoje.

3. Pareiškėja savo telefono numeriu SMS žinute gavo prisijungimo prie paskyros iš kito įrenginio patvirtinimo kodą ir jį suvedė suklastotame interneto puslapyje *www.paeyserra.com*.

Bendrovės teigimu, tokiu būdu pareiškėja šiuo kodu pasidalijo su trečiaisiais asmenimis, dėl to jie įgijo galimybę iš kito įrenginio prisijungti prie pareiškėjos paskyros ir be pareiškėjos žinios ir sutikimo inicijuoti mokėjimo operacijas.

Bendrovės teigimu, jeigu pareiškėja į suklastotą bendrovės interneto puslapį nebūtų suvedusi savo prisijungimo duomenų bei į pareiškėjos mobilųjį telefoną SMS žinute gauto vienkartinio saugos kodo, kuriuo buvo patvirtintas prisijungimas prie pareiškėjos paskyros ir sąskaitos iš kito įrenginio, tretieji asmenys nebūtų galėję prisijungti prie pareiškėjos paskyros ir iš pareiškėjos sąskaitos inicijuoti mokėjimo operacijų.

Bendrovės nuomone, net jeigu pareiškėja buvo nepakankamai atidi ir neatkreipė dėmesio į tai, kad suklastoto interneto puslapio adresas *www.paeyserra.com* akivaizdžiai skiriasi nuo tikrojo bendrovės adreso *www.bank.paysera.com*, jai turėjo sukelti įtarimų *Paysera* SMS žinutė dėl prisijungimo iš naujo įrenginio patvirtinimo, nes jungiantis prie tikrojo bendrovės puslapio iš kito įrenginio bendrovė neprašo į jos interneto svetainę suvesti SMS žinute gauto vienkartinio saugos kodo. Papildomai bendrovė Lietuvos bankui paaiškino, kad „suklastotame *Paysera* internetiniame puslapyje prisijungimo procesas skiriasi nuo prisijungimo proceso prie tikrosios *Paysera* internetinės svetainės. Jungiantis prie sukčių sukurtos svetainės yra prašoma pirmiausiai įvesti vartotojo vardą, tuomet slaptažodį ir SMS žinute gautą saugos kodą. Jungiantis prie tikrosios *Paysera* internetinės svetainės yra prašoma suvesti prisijungimo vardą ir slaptažodį, o jeigu prisijungimas vyksta iš naujo įrenginio, šiuo atveju kompiuterio, prieš suvedant slaptažodį, klientas ekrane yra informuojamas apie prisijungimą iš nepažįstamo įrenginio ir apie būtiną atlikti prisijungimo patvirtinimą. Prisijungimo patvirtinimas atliekamas jau suvedus slaptažodį ir pilnai prisijungus prie *Paysera* paskyros. Prisijungimas patvirtinamas kliento pasirinktu būdu, SMS žinute arba per Paysera mobiliąją programėlę. Jeigu yra jungiamasi iš įrenginio, iš kurio jau buvo jungtasi prie *Paysera* paskyros, papildoma autentifikacija nėra prašoma, taigi, pareiškėjai jungiantis iš jau *Paysera* sistemoje pažįstamo įrenginio prie sukčių suklastotos *Paysera* internetinės svetainės, įtarimų turėjo sukelti ne tik tai, jog jau pirmame prisijungimo etape yra prašoma suvesti SMS žinute gautą saugos kodą, bet ir ta aplinkybė, jog toks saugos kodas apskritai yra prašomas.“ Bendrovė teigė, kad, pareiškėjai neatskleidus minėto vienkartinio kodo, saugesnio autentiškumo patvirtinimo procedūra nebūtų buvusi atlikta.

Pasisakydama dėl pareiškėjos teiginio, kad nebuvo imtasi visų būtinų veiksmų tam, kad būtų laiku užblokuota pareiškėjos sąskaita, bendrovė paaiškino, kad pareiškėja telefonu į bendrovę kreipėsi iš telefono numerio, kuris nebuvo įvestas į bendrovės sistemą, todėl užtruko daugiau laiko identifikuoti pareiškėją. Pareiškėja buvo identifikuota ketvirtą telefoninio pokalbio minutę, tačiau, kai tai buvo padaryta, 3 000 Eur siekianti mokėjimo operacijų suma jau buvo pervesta gavėjui. Bendrovė apribojo pareiškėjos ir gavėjo sąskaitas ir pareiškėjai grąžino 2 600 Eur. Likusios 400 Eur sumos pareiškėjai negalėjo sugrąžinti, nes gavėjas jau buvo inicijavęs dvi mokėjimo operacijas kortele. Bendrovė teigė neturėjusi galimybės sustabdyti šių kortele iš gavėjo sąskaitos inicijuotų mokėjimo operacijų, nes jos buvo inicijuotos dar prieš užblokuojant gavėjo sąskaitą: 2021 m. lapkričio 5 d. 19:06:26 val. ir 2021 m. lapkričio 5 d. 19:06:58 val.

Papildomai bendrovė teigė, kad sąskaita gavėjui bendrovėje buvo atidaryta 2021 m. kovo 22 d. ir per visą laikotarpį nuo paskyros atidarymo iki sukčiavimo atvejo jokia įtartina gavėjo veikla nebuvo užfiksuota. Buvo atliktas tik vienas 20 Eur pervedimas iš kitos gavėjo turimos banko sąskaitos į bendrovės sąskaitą.

Bendrovė remiasi Mokėjimų įstatymo 39 straipsnio 3 dalimi, kurioje įtvirtinta, kad mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai, jeigu jis juos patyrė veikdamas nesąžiningai arba tyčia ar dėl didelio neatsargumo neįvykdęs vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų. Tokiais atvejais šio straipsnio 1 dalyje nustatytas didžiausios nuostolių sumos ribojimas netaikomas.

Atsižvelgdama į pirmiau išdėstytą informaciją, bendrovė prašo atmesti pareiškėjos reikalavimą kaip nepagrįstą.

Susipažinusi su bendrovės Lietuvos bankui pateiktu atsiliepimu, pareiškėja pateikė savo papildomus paaiškinimus dėl bendrovės atsiliepime išdėstytų argumentų. Pareiškėja teigė nesutinkanti su bendrovės atsiliepime nurodytu argumentu, kad bendrovė, pareiškėjai telefonu bendrovei pranešus apie galimai jos prarastus prisijungimo prie paskyros duomenis, ėmėsi visų būtinų veiksmų, kad pareiškėjos sąskaita bendrovėje būtų kuo skubiau užblokuota ir kad tretieji asmenys negalėtų iš pareiškėjos sąskaitos vykdyti mokėjimo operacijų. Pareiškėja teigia, kad, jai kalbantis su bendrovės darbuotoju, bendrovės darbuotojas iš karto neapribojo pareiškėjos

sąskaitos, dėl to, dar tebesitęsiant pokalbiui, iš jos sąskaitos buvo įvykdytos dvi mokėjimo operacijos gavėjui. Pareiškėja teigia, kad, jai pirmą kartą kreipusis į bendrovę iš kito telefono numerio nei registruotas bendrovėje, bendrovės darbuotojas jos paprašė paskambinti bendrovei iš to telefono numerio, kuris yra registruotas bendrovėje. Pareiškėja taip ir padarė, tačiau jai pavyko susisiekti tik su rusų kalba kalbančiu bendrovės darbuotoju, todėl teko dar kartą skambinti bendrovei, kol pavyko susisiekti su anglų kalba kalbančiu darbuotoju. Pareiškėja teigia, kad jos sąskaita buvo apribota tik po gerų 4–5 minučių nuo jos kreipimosi į bendrovę, o gavėjo sąskaita buvo apribota dar vėliau – tik po 8–10 minučių. Pareiškėjos nuomone, jeigu bendrovė būtų skubiau užblokavusi tiek jos, tiek gavėjo sąskaitą, pareiškėja nebūtų paradusi lėšų.

Pareiškėja taip pat teigė, kad yra neteisingas bendrovės atsiliepime nurodytas teiginys, kad bendrovės klientas SMS žinute vienkartinį saugos kodą prisijungimui prie sąskaitos patvirtinti gauna tik jungdamasis iš nepažįstamo įrenginio. Pareiškėja teigia, kad SMS žinute vienkartinį saugos kodą gaudavo ir jungdamasi iš to paties įrenginio, tačiau iš kitos valstybės. Taip ir buvo tą 2021 m. lapkričio 5 dieną, kai pareiškėja prie savo paskyros jungėsi iš JAV, todėl SMS žinute gautas vienkartinis saugos kodas jai nesukėlė įtarimų.

Taip pat pareiškėja pakartojo jau anksčiau išsakytus savo argumentus, kad, jos nuomone, bendrovė, nors ir turėjo informacijos apie tapačias, anksčiau vykusias atakas, nesiėmė jokių veiksmų, kad tokias atakas užkardytų. Bendrovė nesiėmė jokių veiksmų, kad *Google* paieškos sistemoje neatsirastų sukčių suklastotos nuorodos į bendrovės interneto svetainę, bendrovė nesiėmė ir jokių kitų priemonių, kad jos klientai būtų apsaugoti nuo tapačių sukčiavimo atakų.

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

Vadovaujantis Lietuvos banko valdybos 2012 m. sausio 26 d. nutarimu Nr. 03-23 patvirtintų Vartotojų ir finansų rinkos dalyvių ginčų neteisminio sprendimo procedūros Lietuvos banke taisyklių 45 punktu, vartojimo ginčai Lietuvos banke nagrinėjami laikantis rungimosi, ginčų nagrinėjimo operatyvumo, koncentracijos, ekonomiškumo ir bendradarbiavimo principų. Nagrinėdamas ginčą Lietuvos bankas atlieka pateiktų įrodymų vertinimą, kurio pagrindu priimamas sprendimas.

Pareiškėjos ir bendrovės ginčas kilo dėl bendrovės atsisakymo grąžinti pareiškėjai dalį pareiškėjos vardu bendrovėje atidarytoje sąskaitoje atliktų mokėjimo operacijų lėšų. Bendrą mokėjimo operacijų lėšų sumą sudaro 3 000 Eur, tačiau, ginčo byloje turimais duomenimis, bendrovė didžiąją dalį (2 600 Eur) mokėjimo operacijų lėšų pareiškėjai grąžino, todėl nagrinėjamo ginčo atveju spręstina tik dėl bendrovės pareigos pareiškėjai grąžinti likusią 400 Eur sumą, kuri, kaip minėta, yra dalis pareiškėjos ginčijamų mokėjimo operacijų sumos.

Pareiškėja teigia neautorizavusi mokėjimo operacijų, jos atliktos be jos žinios ir sutikimo, todėl prašė bendrovės grąžinti ir likusią bendrovės negrąžintą mokėjimo operacijų lėšų dalį. Bendrovė sutinka, kad mokėjimo operacijos galėjo būti inicijuotos ne pačios pareiškėjos, o neteisėtai veikiančių trečiųjų asmenų. Bendrovė teigia, kad tretieji asmenys iš pareiškėjos galėjo pasisavinti prisijungimo prie pareiškėjos paskyros duomenis ir pareiškėjai SMS žinute į jos bendrovei nurodytą mobiliojo telefono numerį atsiųstą vienkartinį saugos kodą ir taip įgyti galimybę iš kito įrenginio bei IP adreso prisijungti prie pareiškėjos paskyros bendrovėje ir inicijuoti mokėjimo operacijas tik todėl, kad pareiškėja dėl savo didelio aplaidumo neišsaugojo personalizuotų saugos duomenų. Pareiškėja teigia nesutinkanti su bendrovės pozicija, kad dėl pareiškėjos didelio aplaidumo tretieji asmenys galėjo pasisavinti prisijungimo prie pareiškėjos paskyros duomenis ir pareiškėjai SMS žinute į jos bendrovei nurodytą mobiliojo telefono numerį atsiųstą vienkartinį saugos kodą.

Tarp šalių nėra ginčo, kad mokėjimo operacijoms įvykdyti nebuvo duotas pareiškėjos sutikimas, t. y. mokėjimo operacijas tiek bendrovė, tiek pareiškėja pripažįsta neautorizuotomis. Lietuvos bankui pateikti duomenys taip pat leidžia tvirtinti, kad mokėjimo operacijos galėjo būti įvykdytos ne pačios pareiškėjos, o trečiųjų asmenų. Atsižvelgiant į tai, kad iš esmės abi ginčo šalys sutaria, kad mokėjimo operacijos galėjo būti inicijuotos be pareiškėjos žinios ir sutikimo, sprendime toliau nebus analizuojamos su mokėjimo operacijų autorizavimo vertinimu susijusios aplinkybės.

Bendrovė Lietuvos bankui pateikė turimus duomenis apie mokėjimo operacijų atlikimo aplinkybes. Iš pareiškėjos bendrovei pateikto jos naršyklės išrašo matyti, kad 2021 m. lapkričio 5 d. pareiškėja savo kompiuteryje *www.google.de* naršyklėje 18:41 val. (Lietuvos laiku) jungėsi prie suklastotos bendrovės paskyros *www.paeyserra.com*. Bendrovės pateiktais duomenimis, 18:44:52 val. prie pareiškėjos paskyros bendrovėje buvo prisijungta naudojantis IOS įrenginiu ir iš IP adreso Nr. 84.247.51.236 (Prancūzijoje) 18:57:43

val., 19:05:39 val. ir 19:07:04 val. buvo inicijuotos trys mokėjimo operacijos. Turimais duomenimis, iš naršyklės savo kompiuteryje pareiškėja po to, kai prisijungė prie sukčių suklastotos svetainės, 18:51 val. per www.google.de paieškos sistemą antrą kartą jungėsi prie tikrojo bendrovės svetainės puslapio www.bank.paysera.com. Bendrovės pateikti duomenys apie IP adresus, iš kurių buvo jungtasi prie pareiškėjos paskyros, patvirtina, kad 18:51:14 val. prie pareiškėjos paskyros bendrovėje buvo jungtasi iš IP adreso Nr. *duomenys neskelbiami* JAV ir per kompiuterio naršyklę *Mozilla*. Taip pat 18:47:54 val. užfiksuotas prisijungimas prie pareiškėjos paskyros bendrovėje iš *Android* įrenginio iš to paties IP adreso *duomenys neskelbiami* JAV. Šie sistemų išrašai patvirtina pareiškėjos nurodytas aplinkybes, kad ji iš pradžių prie savo paskyros jungėsi per savo mobilųjį telefoną, o vėliau per kompiuterį: „2021 m. lapkričio 5 d. apie 5 min. prieš 19 val. aš prisijungiau prie mano Payseros sąskaitos ir iš pradžių dar savo mobiliajame telefone, per kurį aš prisijungimą aktyvavau, pamačiau, kad kažkas padarė pavedimą 2 000 Eur į man nežinomo žmogaus sąskaitą. Visgi prie mano kompiuterio prisijungus aš to pavedimo nebemačiau ir maniau, kad tai sistemos klaida. Praktiškai tik minutei praėjus 18:57 val. iš mano Paysera sąskaitos buvo pervesta pirma suma 1 000 Eur man nepažįstamam žmogui *Hyppolite Abel Nade*."

Taigi, ginčo bylos duomenys patvirtina, kad pareiškėja savo prisijungimo duomenis prarado 18:41 val. (Lietuvos laiku) jungdamasi prie suklastotos bendrovės paskyros www.paeyserra.com. Iš pirmiau minėtų duomenų yra akivaizdu, kad tuo pačiu metu prie pareiškėjos paskyros buvo jungiamasi iš skirtingose valstybėse registruotų skirtingų IP adresų ir skirtingų įrenginių. Todėl iš šios informacijos galima daryti pagrįstą išvadą, kad galimybę prisijungti prie pareiškėjos paskyros ir sąskaitos bendrovėje turėjo ne tik pati pareiškėja, bet ir tretieji asmenys, kurie prie pareiškėjos paskyros jungėsi iš kito įrenginio ir iš kito IP adreso, registruoto Prancūzijoje. Ginčo byloje turimi duomenys patvirtina, kad tretieji asmenys pareiškėjos duomenis galėjo pasisavinti būtent šiuo momentu pareiškėjai suvedant sukčių suklastotoje svetainėje personalizuotus saugos duomenis, įskaitant SMS žinute gautą vienkartinį saugos kodą.

Kaip ir buvo minėta, tarp ginčo šalių iš esmės nėra ginčo dėl mokėjimo operacijų inicijavimo aplinkybių ir abi ginčo šalys sutinka, kad mokėjimo operacijos buvo inicijuotos be pareiškėjos žinios ir sutikimo tretiesiems asmenims neteistu būdu pasisavinus pareiškėjos prisijungimo prie paskyros duomenis ir SMS žinute gautą vienkartinį saugos kodą. Ginčo šalys iš esmės nesutaria dėl to, kam turėtų tekti atsakomybė už neautorizuotų mokėjimo operacijų įvykdymą: bendrovė teigia, kad pareiškėjos elgesys tretiesiems asmenims atskleidžiant personalizuotus saugos duomenis buvo labai aplaidus, pareiškėja teigia, kad jos elgesys neturi didelio aplaidumo požymių.

Teigdama, kad pareiškėja dėl savo didelio aplaidumo tretiesiems asmenims atskleidė savo personalizuotus saugos duomenis, bendrovė remiasi tuo, kad pareiškėja per www.google.de paieškos sistemą jungdamasi prie bendrovės paskyros nepastebėjo, kad sukčių suklastotas bendrovės interneto svetainės adresas www.paeyserra.com akivaizdžiai skyrėsi nuo bendrovės tikrojo svetainės adreso www.bank.paysera.com ir kad sukčių suklastotoje bendrovės svetainėje suveda SMS žinute gautą vienkartinį saugos kodą, skirtą prisijungimui prie pareiškėjos paskyros patvirtinti. Bendrovės teigimu, kai jungiamasi prie tikros bendrovės paskyros, bendrovė savo paskyroje neprašo suvesti SMS žinute gauto vienkartinio saugos kodo. Pareiškėja teigia, kad jos elgesys nebuvo itin aplaidus, nes suklastota bendrovės svetainė vizualiai atrodė tokia pati, todėl jungdamasi prie suklastotos bendrovės svetainės pareiškėja nieko neįprasto nepastebėjo, be to, SMS žinute gautas vienkartis kodas ir prašymas jį suvesti pareiškėjai nekėlė jokio įtarimo, nes anksčiau ji ne vieną kartą prie savo paskyros jungėsi iš kito įrenginio ir tokį kodą suvesdavo. Priešingai, pareiškėja teigia, kad bendrovė neužtikrino naudojimosi sąskaita saugumo, nes, nors žinojo apie tapačias sukčių atakas prieš bendrovės klientus, nesiėmė jokių priemonių, kad *Google* paieškos sistemoje sukčiai pirmu pasirinkimu neskelbtų sukčių suklastotos nuorodos į bendrovės svetainę. Be to, bendrovė neužtikrino, kad kiekviena mokėjimo operacija būtų papildomai patvirtinama PIN kodo slaptažodžiu.

Siekiant išspręsti tarp bendrovės ir pareiškėjos kilusį ginčą, reikia įvertinti, ar pareiškėjos elgesys, dėl kurio tretiesiems asmenims buvo atskleisti prisijungimo prie pareiškėjos paskyros duomenys, laikytinas labai neatsargiu ar tik neatsargiu. Taip pat svarbu įvertinti ir kitas papildomas pareiškėjos nurodytas aplinkybes, susijusias su bendrovės veiksmais apribojant naudojimąsi pareiškėjos sąskaita bendrovėje bei apribojant gavėjo sąskaitą bendrovėje.

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 Mokėjimų įstatymas.

Dėl neautorizuotų mokėjimo operacijų pasekmių ir pareiškėjos teisės į mokėjimo operacijų sumos grąžinimą

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

Pagal Mokėjimų įstatymo 39 straipsnio 1 dalį, mokėtojui gali tekti dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai iki 50 eurų, 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 jis iki mokėjimo operacijos įvykdymo negalėjo pastebėti mokėjimo priemonės praradimo, vagystės arba neteisėto pasisavinimo, išskyrus atvejus, kai jis veikė nesąžiningai (1 punktas). Mokėjimų įstatymo 39 straipsnio 3 dalyje nustatyta, kad mokėtojui tenka visi dėl neautorizuotų mokėjimo operacijų atsiradę nuostoliai, jeigu jis juos patyrė veikdamas nesąžiningai arba tyčia ar dėl didelio neatsargumo neįvykdęs vienos ar kelių šio įstatymo 34 straipsnyje nustatytų pareigų. Tokiais atvejais Mokėjimų įstatymo 39 straipsnio 1 dalyje nustatytas didžiausios nuostolių sumos ribojimas netaikomas.

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.

Kaip ir minėta, bendrovė teigia, kad tretieji asmenys galėjo pasisavinti pareiškėjos prisijungimo prie paskyros duomenis ir SMS žinute į pareiškėjos mobiliojo telefono numerį atsiųstą vienkartinį saugos kodą, kuriuo prisijungimas prie pareiškėjos sąskaitos iš kito įrenginio buvo patvirtintas tik todėl, kad pareiškėja dėl savo didelio neatsargumo neišsaugojo savo prisijungimo prie paskyros duomenų ir tretiesiems asmenims atskleidė SMS žinute gautą vienkartinį saugos kodą.

Kad būtų galima įvertinti, ar pareiškėja iki mokėjimo operacijos įvykdymo galėjo pastebėti, kad mokėjimo priemonė buvo neteisėtai pasisavinta, svarbūs ne tik bendrovės pateikti sistemų išrašų duomenys apie mokėjimo operacijų įvykdymą, bet ir ginčo šalių paaiškinimai apie mokėjimo priemonės praradimo ir mokėjimo operacijų įvykdymo aplinkybes. Vertinant ginčo šalių pateiktus paaiškinimus apie mokėjimo operacijų atlikimo aplinkybes, matyti, kad iš esmės ginčo šalių paaiškinimai apie aplinkybes, kuriomis tretieji asmenys galėjo pasisavinti prisijungimo prie paskyros duomenis ir be pareiškėjos žinios ir sutikimo inicijuoti mokėjimo operacijas, sutampa. Taip pat ir bendrovės pateikti sistemų išrašai patvirtina pareiškėjos pateiktus paaiškinimus apie mokėjimo operacijų inicijavimo ir įvykdymo aplinkybes.

Kaip minėta, ginčo byloje nustatyta, kad pareiškėja prarado savo prisijungimo prie paskyros duomenis, kai prie paskyros prisijungė per *Google* paieškos sistemą spausdama *Google* paieškos sistemoje reklaminę nuorodą į netikrą bendrovės svetainę *www.paeyserra.com* ir joje suvedė savo prisijungimo prie paskyros duomenis ir SMS žinute gautą vienkartinį saugos kodą. Teigdama, kad pareiškėjos elgesys turi didelio aplaidumo požymių, bendrovė iš esmės remiasi dviem aplinkybėmis: 1. pareiškėja nepastebėjo, kad sukčių suklastotos bendrovės svetainės adresas *www.paeyserra.com* akivaizdžiai skiriasi nuo tikrojo bendrovės svetainės adreso *www.bank.paysera.com*; 2. tikroje bendrovės paskyroje bendrovė neprašo suvesti SMS žinute gauto vienkartinio saugos kodo. Taip pat bendrovė paaiškino, kad SMS žinute gautas vienkartinis saugos kodas, kuriuo patvirtinamas prisijungimas prie paskyros bendrovėje, yra siunčiamas tik tada, kai prie paskyros bandoma prisijungti iš kito, bendrovei nepažįstamo įrenginio. Jeigu prie paskyros jungiamasi iš įrenginio, iš kurio bendrovės paslaugų vartotojas jau buvo jungęsis anksčiau, SMS žinute gautas vienkartinis saugos kodas nėra siunčiamas ir prašomas suvesti. Be to, sukčių suklastotoje bendrovės paskyroje sukčiai SMS žinute gautą vienkartinį saugos kodą prašo suvesti suklastotame bendrovės interneto puslapyje dar tik

jungiantis prie bendrovės paskyros (suvedant prisijungimo vardą, slaptažodį), nors jungiantis prie tikrosios bendrovės paskyros SMS žinute gautas kodas prašomas suvesti tik vėliau, jau esant prisijungus prie paskyros, tačiau dar negalint ja naudotis.

Lietuvos bankas pažymi, kad didelis neatsargumas ar paprastas neatsargumas yra vertinamojo pobūdžio aplinkybės, todėl išvada dėl mokėtojo elgesio vertinimo kaip neatsargaus ar labai neatsargaus dėl neautorizuotos mokėjimo operacijos ar dėl mokėjimo priemonės praradimo, lėmusio neautorizuotą mokėjimo operaciją, darytina kiekvienu konkrečiu atveju, įvertinus 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 neautorizuotos mokėjimo operacijos įvykdymo ir su juo susijusių aplinkybių konteksto.

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

Didelio neatsargumo sąvoka taip pat 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“ (Lietuvos Aukščiausiojo Teismo 2017 m. balandžio 13 d. nutartis civilinėje byloje Nr. e3K-3-180-378/2017, 29 punktas).

Nagrinėjamo ginčo byloje tarp šalių nėra ginčo dėl neautorizuotų mokėjimo operacijų įvykdymo aplinkybių, t. y. tiek pareiškėjos pateikti paaiškinimai apie neautorizuotų mokėjimo operacijų įvykdymo aplinkybes, tiek bendrovės surinkti įrodymai patvirtina, kad pareiškėjos neautorizuotos mokėjimo operacijos buvo inicijuotos pareiškėjai dėl neteisėtų trečiųjų asmenų veiksmų praradus savo mokėjimo priemonę, tai lėmė neautorizuotų mokėjimo operacijų įvykdymą. Ginčo byloje nustatytais duomenimis, tretieji asmenys neteisėtu būdu iš pareiškėjos pasisavino jos mokėjimo priemonę, pareiškėjai per *Google* paieškos sistemą mėginant jungtis prie savo paskyros bendrovėje, paspaudus nuorodą į sukčių suklastotą bendrovės interneto puslapį *www.paeyserra.com* ir joje suvedus savo prisijungimo vardą, slaptažodį bei SMS žinute gautą vienkartinį saugos kodą, kuriuo ir buvo patvirtintas prisijungimas prie pareiškėjos paskyros iš kito įrenginio. Taigi, pareiškėja per *Google* paieškos sistemą mėgindama prisijungti prie savo paskyros bendrovėje nepastebėjo, kad nuorodos į bendrovės svetainės interneto adresą pavadinimas *www.paeyserra.com* skiriasi nuo nuorodos į tikrąjį bendrovės interneto svetainės adresą pavadinimo *www.bank.paysera.com*. Bendrovė teigia, kad sukčių suklastotas bendrovės interneto svetainės adresas *www.paeyserra.com* akivaizdžiai skyrėsi nuo tikrojo bendrovės svetainės adreso *www.bank.paysera.com*, todėl faktas, kad pareiškėja to nepastebėjo, įrodo pareiškėjos didelį aplaidumą.

Vertinant, ar pareiškėjos elgesys, kai ji, mėgindama jungtis per *Google* paieškos sistemą prie savo paskyros bendrovėje nepastebėjo, kad nuoroda į bendrovės svetainės adresą, kurią ji paspaudė, skyrėsi nuo tikrojo bendrovės svetainės adreso, gali būti vertinamas kaip labai aplaidus pareiškėjos elgesys, t. y. toks elgesys, dėl kurio mokėjimo priemonės turėtojo veiksmai iš esmės skiriasi nuo atsargaus elgesio reikalavimų, pažymėtina, kad, Lietuvos banko nuomone, negalima būtų daryti išvados, kad sukčių suklastoto bendrovės interneto svetainės adreso pavadinimas *www.paeyserra.com* ir tikrojo bendrovės svetainės adreso pavadinimas *www.bank.paysera.com* yra akivaizdžiai besiskiriantys, dėl to vartotojui turėtų ir galėtų būti akivaizdu, kad jis jungiasi ne prie savo tikrosios paskyros bendrovėje. Abiejų nuorodų pavadinimuose yra nurodomas bendrovės pavadinimas, skiriasi tik tuo, kad sukčių suklastotame bendrovės interneto svetainės adreso pavadinimo pradžioje nėra žodžio „bank“ ir paties bendrovės pavadinimas nurodytas klaidingai, tačiau vizualiai labai panašiai. Be to, į *Google* paieškos sistemą įvedus bendrovės pavadinimą, kaip pirmas pasirinkimas, yra pateikiama nuoroda į tikrąją bendrovės svetainę adresu *www.paysera.lt*, o kaip antras pasirinkimas pateikiama nuoroda prisijungti prie bendrovės paskyros pavadinimu *www.bank.paysera.com*. Prie paskyros bendrovėje galima prisijungti tiek per bendrovės

nuorodą *www.paysera.lt*, tiek per *www.bank.paysera.com*. Įvertinus šias aplinkybes, galima teigti, kad pareiškėjai sukčių suklastotas bendrovės interneto svetainės adresas *www.paeyserra.com* galėjo ir nesukelti įtarimų, nepaisant to, kad nuorodos pavadinime nebuvo žodžio „bank" ir kad bendrovės pavadinimas buvo nurodytas su klaidomis. Vertinant pareiškėjos elgesį, nebūtų galima teigti, kad pareiškėja, nepastebėdama, kad sukčių suklastotas bendrovės interneto svetainės adresas *www.paeyserra.com* skiriasi nuo tikrojo bendrovės svetainės adreso *www.bank.paysera.com*, buvo labai neatsargi, t.y. kad šis pareiškėjos elgesys buvo toks, dėl kurio pareiškėjos veiksmai iš esmės skyrėsi nuo atsargaus elgesio ir pasireiškė dideliu pareiškėjos aplaidumu. Taigi, Lietuvos banko vertinimu, pareiškėjos elgesio, kai ji per *Google* paieškos sistemą jungdamasi prie savo paskyros bendrovėje nepastebėjo, kad interneto svetainės adreso pavadinimas, prie kurio ji jungėsi, skyrėsi nuo tikrojo bendrovės svetainės adreso, negalima būtų vertinti kaip labai neatsargaus.

Teigdama, kad pareiškėja dėl savo didelio neatsargumo prarado mokėjimo priemonę ir tai lėmė neautorizuotų mokėjimo operacijų įvykdymą, bendrovė remiasi ir aplinkybe, kad pareiškėja sukčių suklastotoje bendrovės svetainėje *www.paeyserra.com* suvedė ne tik savo prisijungimo vardą, slaptažodį, bet ir SMS žinute gautą vienkartinį saugos kodą, skirtą prisijungimui prie pareiškėjos paskyros iš kito įrenginio patvirtinti. Bendrovės teigimu, jungiantis prie tikrosios bendrovės paskyros iš kito įrenginio, bendrovė savo paskyroje neprašo suvesti SMS žinute gauto vienkartinio saugos kodo, todėl pareiškėjai turėjo kilti įtarimas, kodėl jos prašoma SMS žinute gautą vienkartinį saugos kodą suvesti bendrovės paskyroje, taigi, pareiškėja turėjo nesielgti labai neapdariai ir neatlikti šio veiksmo.

Bendrovės Lietuvos bankui pateiktais duomenimis, jungiantis prie sukčių suklastotos netikros bendrovės paskyros iš kito įrenginio, prisijungimo veiksmų seka yra kitokia nei tikrojoje bendrovės aplinkoje. Jungiantis prie sukčių suklastotos bendrovės paskyros, tiek prisijungimo vardą ir slaptažodį, tiek SMS žinute gautą saugos kodą yra prašoma suvesti jau atliekant pirmuosius žingsnius, o jungiantis prie tikrosios bendrovės paskyros iš kito įrenginio pirmiausia prašoma suvesti prisijungimo vardą ir slaptažodį ir tik vėliau, juos suvedus bei patekus į bendrovės paskyrą (tačiau dar negalint ja naudotis), yra prašoma papildomai autentifikuotis (patvirtinti prisijungimą per mobiliąją programėlę arba SMS žinute), jeigu jungiamasi iš kito įrenginio.

Vertinant šias bendrovės nurodytas aplinkybes, svarbu tai, kad, ginčo byloje turimais duomenimis, pareiškėja per *Google* paieškos sistemą prie sukčių suklastotos bendrovės svetainės *www.paeyserra.com* jungėsi iš įrenginio (kompiuterio), kuris bendrovės sistemoms jau buvo pažįstamas, nes pareiškėja iš jo jau buvo jungusis ir anksčiau. Kaip ir minėta, bendrovės pateiktais duomenimis, jungiantis prie bendrovės paskyros iš bendrovei jau pažįstamo įrenginio, papildomai autentifikuotis (patvirtinti prisijungimą per mobiliąją programėlę arba SMS žinute) nėra prašoma, kad patektum į savo paskyrą, pakanka tik suvesti savo prisijungimo vardą bei slaptažodį. Kadangi pareiškėja prie savo paskyros mėgino jungtis iš savo įrenginio, iš kurio ji buvo jungusis jau ir anksčiau, ji galėjo tikėtis, kad tik suvedusi savo prisijungimo vardą bei slaptažodį pateks į savo paskyrą. Pabrėžtina tai, kad nors bendrovė nurodė, kad jungiantis prie tikrosios paskyros bendrovėje iš kito įrenginio pati prisijungimo veiksmų seka yra kitokia (pirmiausia prašoma suvesti prisijungimo vardą ir slaptažodį ir tik juos suvedus bei patekus į bendrovės paskyrą (tačiau dar negalint ja naudotis) yra prašoma papildomai autentifikuotis (patvirtinti prisijungimą per mobiliąją programėlę arba SMS žinute), šiuo atveju svarbi yra ta aplinkybė, kad pati pareiškėja prie savo paskyros bendrovėje mėgino jungtis iš bendrovei jau pažįstamo įrenginio. Vadinasi, pareiškėja negalėjo tikėtis, kad jos prisijungimo veiksmų seka bus tokia pati kaip bendrovės nurodyta prisijungimo prie paskyros iš kito įrenginio seka. Pareiškėja galėjo tikėtis, kad prie savo paskyros prisijungs atlikusi pirmąjį veiksmą – suvedusi prisijungimo vardą ir slaptažodį. Tačiau pareiškėjos dar papildomai buvo prašoma prisijungimą prie paskyros patvirtinti SMS žinute gautu vienkartiniu saugos kodu, nes prie tikrosios pareiškėjos paskyros bendrovėje jungėsi tretieji asmenys, kurie pasisavino iš pareiškėjos prisijungimo prie paskyros duomenis.

Taigi, įvertinus pirmiau minėtas aplinkybes, galima teigti, kad pareiškėjos veiksmų, kuriuos ji anksčiau turėdavo atlikti norėdama prisijungti prie bendrovės paskyros iš bendrovei jau pažįstamo įrenginio, seka ir veiksmų, kuriuos pareiškėjos buvo prašoma atlikti sukčių suklastotoje bendrovės aplinkoje, seka buvo labai panašios. Vienintelis skirtumas, kuris turėjo sukelti pareiškėjai įtarimą, buvo tas, kad jos buvo prašoma sukčių suklastotoje bendrovės aplinkoje suvesti SMS žinute gautą vienkartinį saugos kodą, kuriuo patvirtinamas prisijungimas prie paskyros iš kito įrenginio.

Pareiškėja Lietuvos bankui teigė, kad SMS žinute gauto vienkartinio saugos kodo suvedimas, skirtas pareiškėjos prisijungimui prie savo paskyros iš kito įrenginio patvirtinti, jai buvo įprastas veiksmas, nes ji dažnai prie savo paskyros jungdavosi iš kitų įrenginių ir gaudavo tokias SMS žinutes su vienkartiniu saugos kodu, kuriuo patvirtindavo savo prisijungimą prie paskyros iš kito įrenginio. Tad ir šį kartą nei prašymas jungiantis prie savo paskyros suvesti SMS žinute gautą vienkartinį saugos kodą, nei pačios SMS žinutės gavimas jai nesukėlė jokių įtarimų, priešingai, atrodė įprastas veiksmas, tokius ji dažnai atlikdavo ir anksčiau. Lietuvos bankui pateikti duomenys patvirtina šį pareiškėjos teiginį, t. y. iš pateiktų duomenų matyti, kad pareiškėja prie savo paskyros bendrovėje jungdavosi iš kitų įrenginių ir iš skirtingose valstybėse registruotų IP adresų. Taigi, remiantis pirmiau minėtomis aplinkybėmis, galima teigti, kad pareiškėja suprato SMS žinute gauto vienkartinio saugos kodo paskirtį – patvirtinti prisijungimą prie savo paskyros, ir manė, kad suvesdama SMS žinute gautą vienkartinį saugos kodą jungiasi prie savo paskyros bendrovėje, tačiau nepastebėjo, kad ji jungiasi prie sukčių suklastotos bendrovės interneto paskyros.

Vertinant pareiškėjos elgesio neatsargumo laipsnį, svarbu tai, kad bendrovės Bendrųjų mokėjimo paslaugų teikimo sąlygų privatiems klientams (toliau – Sąlygos) 5.1 papunktyje pareiškėja ir bendrovė buvo sutarusios dėl tokios sąskaitos valdymo tvarkos: „klientas Paysera Sąskaitą gali valdyti internetu, prisijungęs prie savo Paskyros savo prisijungimo vardu ir Slaptažodžiu bei atlikęs papildomo prisijungimo (saugesnio autentiškumo patvirtinimo) procedūrą.“ Vien tik iš šios Sąlygų nuostatos formuluotės galima manyti, kad papildoma autentifikavimo procedūra yra įprastinis veiksmas, kurį vartotojas atlieka siekdamas internetu valdyti savo sąskaitą bendrovėje. Tai, kad siekiant valdyti savo sąskaitą ne visuomet gali reikėti papildomai autentifikuotis ir (arba) kad tai priklauso nuo to, iš kokio įrenginio jungiamasi, iš minėtos Sąlygų nuostatos nėra aišku. Todėl galima vertinti, kad yra normalu, kad pareiškėja, vesdama SMS žinute gautą vienkartinį saugos kodą, galėjo pagrįstai manyti, kad su bendrove sutartu būdu jungiasi prie savo paskyros bendrovėje. Atkreiptinas dėmesys, kad pareiškėja tapo gana gerai parengtos sukčių atakos auka. Pateiktais duomenimis, sukčių suklastotos bendrovės interneto svetainės adresas *www.paeyserra.com* *Google* paieškos sistemoje buvo atsiradęs kaip pirmasis paieškos pasirinkimas, sukčių suklastotas bendrovės interneto svetainės adresas buvo labai panašus į tikrąjį bendrovės interneto svetainės adresą, todėl pareiškėjai galėjo ir nekilti jokių įtarimų, kad ji jungiasi ne prie tikrosios bendrovės paskyros, o prie sukčių suklastotos. Lietuvos banko nuomone, mokėjimo paslaugų teikėjai, be kitų mokėjimo operacijų įvykdymo saugumą užtikrinančių priemonių, turėtų imtis aktyvių veiksmų, kad jų klientai būtų laiku, tinkamai ir aiškiai informuojami apie visas galimas (žinomas) rizikas, susijusias su mokėjimo priemonės paradimu dėl neteisėtų trečiųjų asmenų veiksmų, ypač bendrovei turint informaciją apie prieš bendrovės klientus jau surengtas panašaus pobūdžio sukčių atakas. Nagrinėjamo ginčo atveju bendrovė nepateikė informacijos, kad ji savo klientus, įskaitant ir pareiškėją, būtų informavusi, kad bendrovė savo svetainėje neprašo papildomai suvesti SMS žinute gauto vienkartinio saugos kodo, kuriuo patvirtinamas prisijungimas prie bendrovės sąskaitos iš kito įrenginio, arba kad būtų atkreipusi klientų dėmesį į tai, kad ne visais atvejais bendrovė prašo papildomai autentifikuotis (pvz., jeigu jungiamasi iš bendrovei pažįstamo įrenginio). Lietuvos banko turimais duomenimis, su panašiomis atakomis bendrovės klientai jau buvo susidūrę ir anksčiau dar 2021 m. rugpjūčio mėn., taigi, bendrovei jau buvo žinoma informacija apie prieš jos klientus rengiamas iš esmės tapačias sukčių atakas ir dėl to bendrovės klientai iš savo sąskaitų prarado lėšų. Taigi, Lietuvos banko turimais duomenimis, bendrovė informaciją apie prieš jos klientus vykdomų tapačių sukčių atakų schemas turėjo jau prieš tris mėnesius iki prieš pareiškėją surengtos sukčių atakos, taigi, turėjo pakankamai laiko imtis veiksmų, kad klientai būtų tinkamai ir jiems prieinamu būdu informuoti, kad turi būti itin budrūs jungdamiesi prie savo paskyros ir vykdydami autentifikavimo procedūrą.

Bendrovės Lietuvos bankui pateiktais duomenimis, bendrovė savo klientus apie galimas sukčiavimo atakas prevenciškai informuoja iššokančiais pranešimais bendrovės sistemoje, bendrovės interneto svetainėje ir per mobiliąją programėlę. Bendrovė taip pat paaiškino, kad skelbia informaciją socialiniuose tinkluose, pvz., savo interneto svetainėje skelbia tokią informaciją: „Šiais laikais, kai kiekvienas gali nesunkiai sukurti internetinę svetainę, rizika būti apgautam netikroje banko svetainėje yra ypač didelė. Sukčių internetinis puslapis (angl. *phishing website*) gali atrodyti kone identiškas tikrajam ir suklaidinti net mus pačius. Internetinis sukčiavimas, kai sukuriamas identiškas banko prisijungimo langas, tampa itin dažnu, ir vienintelis būdas pastebėti skirtumą yra atkreipti dėmesį ir atidžiai perskaityti interneto svetainės adresą.“ Taigi, iš esmės pati bendrovė pripažįsta, kad yra labai didelė rizika

jos vartotojui patekti į sukčių ataką ir būti apgautam sukčiams sukūrus netikrą bendrovės interneto svetainę, ir teigia, kad net ir pačią bendrovę gali suklaidinti sukčių suklastoto bendrovės interneto puslapio panašumas į tikrąjį bendrovės interneto puslapį. Vadinasi, bendrovė pripažįsta, kad ne tik jos klientui, bet ir jai pačiai gali būti sudėtinga atskirti sukčių suklastotą bendrovės interneto svetainę nuo tikrosios. Tačiau, įvertinus bendrovės Lietuvos bankui pateiktus duomenis apie bendrovės klientams skelbiamas žinutes, kuriomis siekiama klientus apsaugoti nuo panašių sukčiavimo atvejų rizikos, kuri, anot bendrovės, yra labai didelė, galima teigti, kad bendrovė deda nepakankamai pastangų tam, kad informacija apie galimą sukčiavimo riziką pasiektų jos klientus ir kad klientų dėmesys būtų atkreiptas į jų atliekamų veiksmų riziką. Kadangi, kaip ir pati bendrovė iš esmės pripažįsta, sukčių suklastotą bendrovės interneto svetainę atskirti nuo tikrosios yra sunku, kad egzistuoja didelė sukčiavimo ir nuostolių patyrimo rizika, darytina išvada, kad bendrovė, suprasdama šią riziką, turėtų dėti daugiau pastangų, kad jos klientai būtų išsamiai informuoti apie galimą sukčiavimo riziką ir kaip nuo to apsisaugoti, taip pat kad ši informacija bendrovės klientus pasiektų.

Atsižvelgiant į pirmiau nurodytas aplinkybes, negalima teigti, kad pareiškėjos elgesys, dėl kurio ji prarado savo mokėjimo priemonę, gali būti pripažįstamas kaip elgesys, pasireiškęs neprotingumu ar išskirtiniu rūpestingumo nebuvimu. Lietuvos banko vertinimu, sukčių suklastota bendrovės paskyra iš esmės ir akivaizdžiai nesiskyrė nuo tikrosios bendrovės paskyros, kaip pati bendrovė nurodė, sukčių paskyrą atskirti nuo tikrosios bendrovės paskyros gali būti ir pačiai bendrovei sudėtinga, pareiškėjos atliekamų veiksmų seka jungiantis prie suklastotos bendrovės paskyros ir jungiantis prie tikrosios bendrovės paskyros iš to paties įrenginio iš esmės nesiskyrė, priešingai, buvo panaši, skyrėsi tik tuo, kad bendrovės tikroje svetainėje nėra prašoma suvesti SMS žinute gauto vienkartinio saugos kodo, o pačios SMS žinutės suvedimas su saugos kodu į sukčių suklastotą bendrovės interneto svetainę pareiškėjai galėjo atrodyti kaip įprastai atliekamas veiksmas, kurį pareiškėja atlikdavo jungdamasi prie savo paskyros. Lietuvos banko nuomone, įvertinus pirmiau išdėstytas ginčo byloje nustatytas aplinkybes ir padarytas išvadas, galima teigti, kad pareiškėja iki mokėjimo operacijos įvykdymo negalėjo pastebėti, kad jos mokėjimo priemonę pasisavino tretieji asmenys. Mokėjimų įstatymo 39 straipsnio 2 dalyje nustatyta, kad mokėtojas neturi patirti jokių nuostolių, jeigu jis iki mokėjimo operacijos įvykdymo negalėjo pastebėti mokėjimo priemonės praradimo, vagystės arba neteisėto pasisavinimo, išskyrus atvejus, kai jis veikė nesąžiningai (1 punktas).

Vertinant Mokėjimų įstatymo nuostatas reglamentuojančias atsakomybės už neautorizuotų mokėjimo operacijų įvykdymą pasiskirstymą, tam, kad bendrovė būtų atleista nuo pareigos grąžinti neautorizuotų mokėjimo operacijų lėšas, turėtų būti nustatytas pareiškėjos sukčiavimas arba didelis neatsargumas. Kaip ir buvo minėta, Lietuvos banko nuomone, nagrinėjamo ginčo atveju pareiškėjos elgesys, dėl kurio ji prarado savo mokėjimo priemonę, negali būti laikomas labai neatsargiu, o apie galimą pareiškėjos sukčiavimą ar kitokį nesąžiningą veikimą ginčo byloje duomenų nėra. Įvertinus pirmiau išdėstytą informaciją, konstatuotina, kad pagrindo pareiškėjai taikyti Mokėjimų įstatymo 39 straipsnio 3 dalį nėra. Kitų aplinkybių, kurios leistų pagrįstai manyti, kad pareiškėjai turėtų tekti visi su neautorizuotomis mokėjimo operacijomis susiję nuostoliai, ginčo byloje taip pat nenustatyta, todėl, Lietuvos banko vertinimu, pareiškėjos reikalavimas bendrovei grąžinti ir likusią dalį neautorizuotų mokėjimo operacijų lėšų sumos yra pagrįstas, todėl tenkintinas.

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

Pareiškėja teigia, kad bendrovė, pareiškėjai kreipusis telefonu ir pranešus apie savo mokėjimo priemonės paradimą ir neautorizuotą jos panaudojimą, nesiėmė visų veiksmų tam, kad nedelsiant būtų apribotas naudojimasis pareiškėjos sąskaita.

Mokėjimų įstatymo 39 straipsnio 5 dalyje nustatyta, kad „mokėtojas neturi patirti jokių nuostolių dėl prarastos, pavogtos ar neteisėtai pasisavintos mokėjimo priemonės po to, kai pateikia šio įstatymo 34 straipsnio 1 dalies 2 punkte nurodytą pranešimą, išskyrus atvejus, kai jis veikė nesąžiningai“. Mokėjimų įstatymo 34 straipsnio 1 dalies 2 punkte nurodoma, kad mokėtojas, sužinojęs apie mokėjimo priemonės praradimą, vagystę arba neteisėtą pasisavinimą ar neautorizuotą jos naudojimą, nedelsdamas apie tai turi pranešti mokėjimo paslaugų teikėjui arba jo nurodytam subjektui. Mokėjimų įstatymo 39 straipsnio 6 dalyje nustatyta, kad „jeigu mokėjimo paslaugų teikėjas nesudaro sąlygų bet kuriuo metu pranešti apie prarastą, pavogtą arba neteisėtai pasisavintą mokėjimo priemonę, nuostoliai, atsiradę dėl mokėjimo priemonės neautorizuoto naudojimo, tenka mokėjimo paslaugų teikėjui, išskyrus

atvejus, kai mokėtojas veikė nesąžiningai“.

Ginčo byloje nustatytais duomenimis, pareiškėja savo prisijungimo prie paskyros duomenis prarado 2021 m. lapkričio 5 d. 18:41 val. (Lietuvos laiku), o į bendrovę telefonu kreipėsi 2021 m. lapkričio 5 d. 19:02:50 val. Bendrovė pareiškėjos tapatybę nustatė apie 19:11–19:12 val., o pareiškėjos sąskaitą apribojo 19:12:13 val. Pareiškėjos neautorizuotos mokėjimo operacijos buvo įvykdytos 18:57:43 val., 19:05:39 val. ir 19:07:04 val. Taigi, pirma mokėjimo operacija buvo įvykdyta iki pareiškėjos kreipimosi į bendrovę ir pranešimo apie mokėjimo priemonės paradimą ir neautorizuotą jos panaudojimą, o dvi paskesnės buvo įvykdytos pareiškėjai telefonu kalbantis su bendrovės darbuotoju ir bendrovės darbuotojui nesėkmingai mėginant nustatyti pareiškėjos tapatybę.

Bendrovė pateikė pareiškėjos ir bendrovės pokalbio įrašus, iš kurių matyti, kad bendrovės darbuotojas, pareiškėjai kreipusis į bendrovę telefonu, mėgino nustatyti pareiškėjos tapatybę. Turimais duomenimis, šis pokalbis truko iš viso 5 min 52 sek. (nuo 19:02:50 val. iki 19:08:42 val.). Iš pateikto pokalbio įrašo matyti, kad bendrovės darbuotojas pareiškėjai paaiškino, kad ji bendrovei skambina iš telefono numerio, kuris nėra registruotas bendrovės sistemoje, todėl bendrovės darbuotojas negali pareiškėjos iš karto identifikuoti, ir pasisiūlė pareiškėjai paskambinti į tą telefono numerį, kuris yra registruotas bendrovės sistemoje arba pačiai pareiškėjai perskambinti bendrovei iš to telefono numerio, kuris buvo nurodytas bendrovės sistemoje, arba pareiškėjos telefono numerį, iš kurio ji skambino bendrovei, užregistruoti bendrovės sistemoje. Iš pateikto pokalbio įrašo matyti, kad pareiškėja bandė naują telefono numerį užregistruoti bendrovės sistemoje, tačiau, to padaryti nepavykus, bendrovės darbuotojas 19:10:32 val. pareiškėjai paskambino į tą telefono numerį, kuris buvo registruotas bendrovės sistemoje, ir šio pokalbio metu bendrovės darbuotojas per pirmąsias pokalbio minutes nustatė pareiškėjos tapatybę ir apribojo naudojimąsi pareiškėjos sąskaita. Taigi, remiantis pirmiau minėtais ginčo byloje turimais duomenimis, dvi mokėjimo operacijos buvo įvykdytos pirmo pokalbio su bendrovės darbuotoju metu, kai buvo mėginama nustatyti pareiškėjos tapatybę tam, kad būtų apribotas naudojimasis jos sąskaita.

Vertinant, ar bendrovė nepagrįstai ilgai delsė apriboti pareiškėjos sąskaitą nuo momento, kai pareiškėja bendrovę informavo apie savo mokėjimo priemonės paradimą ir neautorizuotą jos panaudojimą, o bendrovė nustačiusi pareiškėjos tapatybę apribojo naudojimąsi sąskaita, svarbu atkreipti dėmesį į tai, kad nuo tada, kai bendrovė nustatė pareiškėjos tapatybę ir apribojo naudojimąsi pareiškėjos sąskaita, praėjo tik apytiksliai 2 minutės. Objektyviai vertinant negalima teigti, kad toks laiko tarpas galėtų būti pripažintas kaip nepagrįstai ilgas delsimas. Be to, pareiškėja mokėjimo priemonę buvo praradusi dar anksčiau, t. y. 18:41 val., tad tretieji asmenys iki pareiškėjai kreipiantis į bendrovę jau buvo įgiję galimybę naudotis pareiškėjos sąskaita ir iš jos vykdyti mokėjimo operacijas.

Vertinant, ar bendrovės darbuotojas pirmo pokalbio metu nepagrįstai ilgai delsė nustatyti pareiškėjos tapatybę, svarbu tai, kad pokalbio metu bendrovės darbuotojas pirmiausia pats pasisiūlė pareiškėjai perskambinti bendrovės sistemoje registruotu pareiškėjos telefono numeriu tam, kad greičiau ir paprasčiau galėtų identifikuoti pareiškėją, tačiau, pareiškėjai nesutikus, bendrovės darbuotojas pareiškėjai pasiūlė pačiai iš naujo perskambinti bendrovei iš telefono numerio, registruoto bendrovėje, arba užregistruoti naują telefono numerį bendrovės sistemoje. Kaip ir buvo minėta, pareiškėja rinkosi pastarąjį variantą, kuris pagal proceso trukmę yra pats ilgiausias. Tik nepavykus naujo telefono numerio užregistruoti bendrovės sistemoje, pareiškėja sutiko, kad bendrovės darbuotojas pats jai paskambintų. Taigi, įvertinus Lietuvos bankui pateikto pokalbio įrašą, galima teigti, kad pirmo pokalbio metu iš karto identifikuoti pareiškėjos tapatybės nepavyko ir dėl pačios pareiškėjos veiksmų, nes ji iš esmės pasirinko patį ilgiausią identifikavimo proceso variantą. Įvertinus Lietuvos bankui pateiktą pokalbio įrašą, negalima teigti, kad pirmo pokalbio su bendrovės darbuotoju metu pareiškėja nebuvo identifikuota dėl kokių nors aplaidžių bendrovės darbuotojo veiksmų, todėl nėra pagrindo teigti, kad bendrovė pareiškėjai nesudarė galimybių bet kuriuo metu pranešti apie prarastą, pavogtą arba neteisėtai pasisavintą mokėjimo priemonę.

Įvertinus pirmiau nustatytą informaciją, galima teigti, kad dvi pareiškėjos neautorizuotos mokėjimo operacijos buvo įvykdytos tada, kai pareiškėja pranešė apie mokėjimo priemonės paradimą ir neautorizuotą jos panaudojimą, o bendrovės darbuotojas bandė nustatyti pareiškėjos tapatybę. Svarbu tai, kad, mokėjimo paslaugų teikėjui gavus jo paslaugų vartotojo pranešimą apie mokėjimo priemonės paradimą ir neautorizuotą jos panaudojimą, objektyviai yra reikalingas tam tikras laiko tarpas tam, kad būtų identifikuotas vartotojas ir būtų imtasi priemonių, kad būtų apribotas naudojimasis mokėjimo priemone.

Nagrinėjamo ginčo atveju nėra pagrindo teigti, kad bendrovė nepagrįstai ilgai delsė apriboti naudojimąsi pareiškėjos sąskaita arba kad nesudarė pareiškėjai galimybių nedelsiant pranešti apie mokėjimo priemonės paradimą ir neautorizuotą jos panaudojimą. Taip pat nėra pagrindo teigti, kad dvi pareiškėjos neautorizuotos mokėjimo operacijos buvo įvykdytos po to, kai buvo pranešta apie mokėjimo priemonės paradimą ir neautorizuotą jos panaudojimą, nes, kaip ir buvo minėta, šios mokėjimo operacijos buvo įvykdytos tada, kai pranešimas buvo teikiamas ir buvo tikrinama informacija.

Remdamasis tuo, kas išdėstyta, ir vadovaudamasis Vartotojų teisių apsaugos įstatymo 27 straipsnio 1 dalies 1 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 59.1 papunkčiu, n u s p r e n d ž i u:

1. Tenkinti pareiškėjos X.X. reikalavimą ir rekomenduoti bendrovei grąžinti pareiškėjai 400 Eur.

2. Įpareigoti bendrovę per mėnesį nuo šio sprendimo priėmimo dienos raštu informuoti Lietuvos banką apie šio sprendimo rezoliucinės dalies 1 punkte nurodytos rekomendacijos įgyvendinimą (neįgyvendinimą). Bendrovei neįvykdžius minėtos rekomendacijos, apie tai bus paskelbta Lietuvos Respublikos teisės aktų nustatyta tvarka.

Lietuvos banko sprendimas dėl ginčo esmės yra rekomendacinio pobūdžio ir teismui neskundžiamas. Vartotojui ir finansų rinkos dalyviui išlieka teisė dėl tapataus ginčo dalyko kreiptis į teismą arba kitą ginčų nagrinėjimo instituciją įstatymų nustatyta tvarka. Kreipimasis į teismą po Lietuvos banko sprendimo dėl ginčo esmės priėmimo nelaikomas šio Lietuvos banko sprendimo apskundimu. Ginčo šalys turi pareigą pranešti Lietuvos bankui, jeigu viena iš ginčo šalių pareiškia ieškinį bendrosios kompetencijos teismui, prašydama nagrinėti tapatų ginčą iš esmės.

Direktorius Arūnas Raišutis