KOMISIJOS DELEGUOTASIS REGLAMENTAS (ES) 2018/389

2017 m. lapkričio 27 d.

kuriuo Europos Parlamento ir Tarybos direktyva (ES) 2015/2366 papildoma griežto kliento autentiškumo patvirtinimo ir bendrų ir saugių atvirųjų ryšių standartų techniniais reguliavimo standartais

(Tekstas svarbus EEE)

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2015 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyvą (ES) 2015/2366 dėl mokėjimo paslaugų vidaus rinkoje, kuria iš dalies keičiamos direktyvos 2002/65/EB, 2009/110/EB ir 2013/36/ES bei Reglamentas (ES) Nr. 1093/2010 ir panaikinama Direktyva 2007/64/EB ([1]), ypač į jos 98 straipsnio 4 dalies antrą pastraipą,

kadangi:

(1) elektroniniu būdu siūlomos mokėjimo paslaugos turėtų būti teikiamos saugiai, įdiegiant technologijas, kuriomis galima užtikrinti saugų vartotojo autentiškumo patvirtinimą ir kuo labiau sumažinti sukčiavimo riziką. Apskritai 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 paslaugų vartotojas, įprastu būdu nurodęs personalizuotus saugumo požymius, būtų teisėtas vartotojas ir kaip toks išreikštų savo sutikimą pervesti lėšas ir gauti informaciją apie jo sąskaitą. Be to, būtina nustatyti griežto kliento autentiškumo patvirtinimo reikalavimus, taikytinus kas kartą, kai mokėtojas internetu prisijungia prie savo mokėjimo sąskaitos, inicijuoja elektroninę mokėjimo operaciją arba nuotolinio ryšio priemone vykdo bet kokį veiksmą, kuris gali būti susijęs su sukčiavimo atliekant mokėjimą ar kitokio piktnaudžiavimo rizika, reikalaujant sukurti atpažinties kodą, kurio būtų neįmanoma padirbti nei viso, nei atskleidus kuriuos nors elementus, naudotus jį kuriant;

(2) nuolat kintant sukčiavimo metodams, griežto kliento autentiškumo patvirtinimo reikalavimais turėtų būti numatomos techninių sprendimų inovacijos reaguojant į atsiradusias naujas grėsmes elektroninių mokėjimų saugumui. Siekiant užtikrinti, kad nustatytini reikalavimai būtų veiksmingai ir nepertraukiamai įgyvendinami, taip pat derėtų įpareigoti griežto kliento autentiškumo patvirtinimo taikymo saugumo priemones ir jo išimtis, personalizuotų saugumo požymių konfidencialumo ir vientisumo apsaugos priemones ir bendrų ir saugių atvirųjų ryšių standartų priemones dokumentuoti, reguliariai testuoti ir vertinti, be to, jų auditą turėtų atlikti veiklos požiūriu nepriklausomi auditoriai, turintys IT saugumo ir mokėjimų srities kompetencijos. Tam, kad kompetentingos institucijos galėtų stebėti šių priemonių peržiūros kokybę, tokių peržiūrų duomenys turėtų paprašius būti joms pateikiami;

(3) kadangi elektroninėms nuotolinėms mokėjimo operacijoms kyla didesnė sukčiavimo rizika, tokioms operacijoms būtina nustatyti papildomus griežto kliento autentiškumo patvirtinimo reikalavimus, užtikrinant dinamišką operacijos susiejimą su suma ir gavėju, kuriuos inicijuodamas operaciją nurodė mokėtojas;

(4) dinamiškas susiejimas yra galimas kuriant atpažinties kodus, kuriems taikomi griežti saugumo reikalavimai. Siekiant neutralumo technologiniu požiūriu, nereikėtų įpareigoti taikyti konkrečių atpažinties kodų vykdymo technologijų. Todėl atpažinties kodai turėtų būti grindžiami tokiais sprendimais, kaip vienkartinių slaptažodžių kūrimas ir patvirtinimas, skaitmeninis parašas ar kitoks kriptografinis galiojimo patvirtinimas naudojant raktus arba kriptografinę medžiagą, saugomus autentiškumo patvirtinimo elementuose, jeigu laikomasi saugumo reikalavimų;

([1]) OL L 337, 2015 12 23, p. 35.

(5) būtina nustatyti konkrečius reikalavimus atvejams, kai mokėtojui inicijuojant elektroninę nuotolinę mokėjimo operaciją galutinė suma nėra žinoma, siekiant užtikrinti, kad griežtas kliento autentiškumo patvirtinimas konkrečiai galioja didžiausiai sumai, kuriai mokėtojas yra davęs leidimą, kaip nurodoma Direktyvoje (ES) 2015/2366;

(6) siekiant užtikrinti, kad griežtas kliento autentiškumo patvirtinimas būtų taikomas, taip pat būtina nustatyti tinkamas apsaugos savybes, privalomas griežto kliento autentiškumo patvirtinimo elementams, priskiriamiems prie tokių kategorijų, kaip žinojimas (tai, ką žino tik vartotojas), pavyzdžiui, trukmė ar sudėtingumas, ir turėjimas (tai, ką turi tik vartotojas), pavyzdžiui, algoritmo specifikacijos, rakto ilgis ir informacijos entropija, ir prietaisams bei programinei įrangai, kuriais nuskaitomi elementai, priskiriami prie būdingumo kategorijos (tai, kas būdinga vartotojui), pavyzdžiui, algoritmo specifikacijos, biometriniai jutikliai ir formų apsaugos savybės, visų pirma siekiant sumažinti šių elementų sužinojimo ir atskleidimo riziką ir pavojų, kad juos panaudos neturinčios leidimo šalys. Be to, būtina nustatyti reikalavimus, kuriais būtų užtikrintas šių elementų nepriklausomumas, kad pažeidus vieną nebūtų paveiktas kitų patikimumas, visų pirma tais atvejais, kai kurie nors iš šių elementų yra naudojami universaliame prietaise, konkrečiai tokiame prietaise kaip planšetinis kompiuteris arba mobilusis telefonas, kuriais galima naudotis tiek teikiant nurodymus atlikti mokėjimą, tiek patvirtinant autentiškumą;

(7) griežto kliento autentiškumo patvirtinimo reikalavimai taikomi mokėtojo inicijuotiems mokėjimams, nepriklausomai nuo to, ar mokėtojas yra fizinis, ar juridinis asmuo;

(8) mokėjimams anoniminėmis mokėjimo priemonėmis dėl paties jų pobūdžio griežto kliento autentiškumo patvirtinimo pareiga netaikytina. Sutartiniu ar teisiniu pagrindu tokių priemonių anonimiškumą panaikinus, mokėjimams pradedami taikyti saugumo reikalavimai pagal Direktyvą (ES) 2015/2366 ir šį techninį reguliavimo standartą;

(9) pagal Direktyvą (ES) 2015/2366 griežto kliento autentiškumo patvirtinimo principo taikymo išimtys nustatytos pagal mokėjimo operacijos rizikos lygį, sumą, jos vykdymo pasikartojimo dažnumą ir mokėjimo kanalą;

(10) veiksmai, susiję su prieiga prie mokėjimo sąskaitos likučio ir paskutinių operacijų, neatskleidžiant neskelbtinų mokėjimo duomenų, pasikartojantys mokėjimai tiems patiems gavėjams, kurių duomenys buvo įvesti anksčiau arba kurie buvo mokėtojo patvirtinti pagal griežto kliento autentiškumo patvirtinimo procedūrą, ir mokėjimai iš tų pačių fizinių ar juridinių asmenų, kurių sąskaitas tvarko tas pats mokėjimo paslaugų teikėjas, ir tiems patiems asmenims laikomi mažai rizikingais, todėl mokėjimo paslaugų teikėjams leidžiama jiems griežto kliento autentiškumo patvirtinimo netaikyti. Nepaisant to, pagal Direktyvos (ES) 2015/2366 65, 66 ir 67 straipsnius mokėjimo inicijavimo paslaugų teikėjai, mokėjimo paslaugų teikėjai, išleidžiantys kortele grindžiamas mokėjimo priemones, ir informavimo apie sąskaitas paslaugų teikėjai konkrečios mokėjimo paslaugos įvykdymui turėtų prašyti ir gauti reikalingą pagrindinę informaciją iš sąskaitą tvarkančio mokėjimo paslaugų teikėjo tik gavę mokėjimo paslaugų vartotojo sutikimą. Toks sutikimas gali būti suteikiamas atskirai kiekvienam informacijos prašymui arba kiekvienam inicijuotinam mokėjimui, arba kaip įgaliojimas informavimo apie sąskaitas paslaugų teikėjams dėl nurodytų mokėjimo sąskaitų ir susijusių mokėjimo operacijų, nustatytų sutartyje su mokėjimo paslaugų vartotoju;

(11) išimtys, taikomos mažos vertės bekontakčiams mokėjimams pardavimo vietose, kai taip pat atsižvelgiama į didžiausią skaičių operacijų iš eilės arba tam tikrą nustatytą didžiausią operacijų iš eilės vertę netaikant griežto kliento autentiškumo patvirtinimo, sudaro sąlygas plėtoti vartotojams palankias ir mažos rizikos mokėjimo paslaugas, todėl tokios išimtys turėtų būti numatytos. Be to, derėtų nustatyti išimtį atvejui, kai elektroninės mokėjimo operacijos inicijuojamos neprižiūrimuose terminaluose, kur vykdyti griežtą kliento autentiškumo patvirtinimą ne visada gali būti lengva dėl operacinių priežasčių (pvz., siekiant išvengti eilių ir galimų nelaimingų atsitikimų ties rinkliavos punktais arba dėl kitų saugumo ar saugos pavojų);

(12) kaip ir išimčių mažos vertės bekontakčiams mokėjimams pardavimo vietose atveju, reikėtų siekti tinkamos pusiausvyros tarp intereso užtikrinti didesnį nuotolinių mokėjimų saugumą ir poreikio e. prekybos srityje sudaryti sąlygas vykdyti vartotojams patogius ir prieinamus mokėjimus. Laikantis šių principų, ribos, kurių nesiekiant nebūtina taikyti griežto kliento autentiškumo patvirtinimo, turėtų būti nustatomos apdairiai ir taikomos tik mažos vertės pirkiniams internetu. Pirkinių internetu vertės ribos turėtų būti nustatomos apdairiau dėl šiek tiek didesnės rizikos saugumui, kadangi asmuo fiziškai nedalyvauja pirkimo metu;

(13) griežto kliento autentiškumo patvirtinimo reikalavimai taikomi mokėtojo inicijuotiems mokėjimams, nepriklausomai nuo to, ar mokėtojas yra fizinis, ar juridinis asmuo. Daugelis įmonių mokėjimų yra inicijuojami taikant specialius procesus ar protokolus, užtikrinančius aukšto lygio mokėjimų saugumą, kurio siekiama pagal Direktyvą (ES) 2015/2366 taikant griežtą kliento autentiškumo patvirtinimą. Jeigu kompetentingos institucijos nustato, kad tie mokėjimų procesai ir protokolai, prieinami tik mokėtojams, kurie nėra vartotojai, saugumo požiūriu atitinka Direktyvos (ES) 2015/2366 tikslus, mokėjimo paslaugų teikėjams gali būti leista tiems procesams ar protokolams netaikyti griežto kliento autentiškumo patvirtinimo;

(14) tuo atveju, kai realiuoju laiku atlikus operacijos rizikos analizę mokėjimo operacija priskiriama prie mažos rizikos operacijų, taip pat derėtų nustatyti išimtį mokėjimo paslaugų teikėjui, kuris ketina netaikyti griežto kliento autentiškumo patvirtinimo, nes pasitvirtina veiksmingus rizika grindžiamus reikalavimus, kuriais užtikrinamas mokėjimo paslaugų vartotojo lėšų ir asmens duomenų saugumas. Šie rizika grindžiami reikalavimai turėtų apimti rizikos analizės rezultatus, kuriais patvirtinama, kad nėra mokėtojui nebūdingų išlaidų arba elgsenos modelių, atsižvelgiant į kitus rizikos veiksnius, pavyzdžiui, mokėtojo ir gavėjo buvimo vietą, ir pinigines ribas, grindžiamas nuotoliniams mokėjimams apskaičiuotais sukčiavimo rodikliais. Kai remiantis realiuoju laiku atlikta operacijos rizikos analize nustatoma, kad mokėjimas negali būti laikomas mažai rizikingu, mokėjimo paslaugų teikėjas turėtų taikyti griežtą kliento autentiškumo patvirtinimą. Didžiausia tokių rizika grindžiamų išimčių vertė turėtų būti nustatyta taip, kad būtų užtikrintas labai mažas atitinkamas sukčiavimo rodiklis, taip pat lyginant su visų mokėjimo paslaugų teikėjo mokėjimo operacijų, įskaitant tas, kurioms taikytas griežtas kliento autentiškumo patvirtinimas, sukčiavimo rodikliais per tam tikrą laikotarpį ir paskutinį ketvirtį;

(15) siekiant veiksmingo vykdymo užtikrinimo, mokėjimo paslaugų teikėjai, pageidaujantys pasinaudoti griežto kliento autentiškumo patvirtinimo išimtimi, turėtų reguliariai stebėti ir gavę prašymą nurodyti kompetentingoms institucijoms ir Europos bankininkystės institucijai (EBI) kiekvienos rūšies mokėjimo operacijų nesąžiningų ar neautorizuotų mokėjimo operacijų vertę ir užfiksuotus visų savo mokėjimo operacijų sukčiavimo rodiklius, nepriklausomai nuo to, ar jų autentiškumas patvirtintas taikant griežtą kliento autentiškumo patvirtinimą, ar jos vykdytos taikant atitinkamą išimtį;

(16) šie surinkti nauji ankstesnių laikotarpių duomenys, susiję su elektroninių mokėjimo operacijų sukčiavimo rodikliais, taip pat padės EBI veiksmingai peržiūrėti griežto kliento autentiškumo patvirtinimo išimties, grindžiamos realiuoju laiku atlikta operacijos rizikos analize, ribas. Pagal Direktyvos (ES) 2015/2366 98 straipsnio 5 dalį ir Europos Parlamento ir Tarybos reglamento (ES) Nr. 1093/2010 ([1]) 10 straipsnį, siekdama didinti nuotolinių elektroninių mokėjimų saugumą, EBI turėtų peržiūrėti šiuos techninius reguliavimo standartus ir atnaujintus jų projektus pateikti Komisijai, jei reikia, pateikdama naujus ribų ir atitinkamų sukčiavimo rodiklių projektus;

(17) mokėjimo paslaugų teikėjams, taikantiems bet kurią nuostatose numatytiną išimtį, turėtų būti leista bet kuriuo metu nuspręsti veiksmams ir mokėjimo operacijoms, kurios tose nuostatose nurodomos, taikyti griežtą kliento autentiškumo patvirtinimą;

(18) priemonėmis, kuriomis apsaugomas personalizuotų saugumo požymių konfidencialumas ir vientisumas, taip pat atpažinties prietaisais ir programine įranga turėtų būti sumažinta sukčiavimo, vykdomo neautorizuotai ar nesąžiningai naudojantis mokėjimo priemonėmis ir įgyjant neautorizuotą prieigą prie mokėjimo sąskaitų, rizika. Todėl būtina nustatyti reikalavimus, taikomus saugiam personalizuotų saugumo požymių kūrimui bei pateikimui ir jų susiejimui su mokėjimo paslaugų vartotoju, ir numatyti tų požymių atnaujinimo ir deaktyvacijos sąlygas;

(19) siekiant užtikrinti veiksmingus ir saugius atitinkamų dalyvių ryšius teikiant informavimo apie sąskaitas paslaugas, mokėjimo inicijavimo paslaugas ir lėšų pakankamumo patvirtinimą, būtina nustatyti bendrų ir saugių atvirųjų ryšių standartų reikalavimus, kurių turėtų laikytis visi atitinkami mokėjimo paslaugų teikėjai. Direktyva (ES) 2015/2366 numatyta, kad informavimo apie sąskaitas paslaugų teikėjai turi prieigą prie mokėjimo sąskaitos informacijos ir gali ja naudotis. Todėl šiuo reglamentu nekeičiamos prieigos prie sąskaitų, išskyrus mokėjimo sąskaitas, taisyklės;

([1]) 2010 m. lapkričio 24 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1093/2010, kuriuo įsteigiama Europos priežiūros institucija (Europos bankininkystės institucija), iš dalies keičiamas Sprendimas Nr. 716/2009/EB ir panaikinamas Komisijos sprendimas 2009/78/EB (OL L 331, 2010 12 15, p. 12).

(20) visi sąskaitas tvarkantys mokėjimo paslaugų teikėjai, turintys internetu pasiekiamų mokėjimo sąskaitų, turėtų pateikti bent vieną prieigos sąsają, užtikrinančią saugius ryšius su informavimo apie sąskaitas paslaugų teikėjais, mokėjimo inicijavimo paslaugų teikėjais ir mokėjimo paslaugų teikėjais, išleidžiančiais kortele grindžiamas mokėjimo priemones. Sąsaja turėtų sudaryti sąlygas informavimo apie sąskaitas paslaugų teikėjams, mokėjimo inicijavimo paslaugų teikėjams ir mokėjimo paslaugų teikėjams, išleidžiantiems kortele grindžiamas mokėjimo priemones, identifikuotis sąskaitą tvarkančio mokėjimo paslaugų teikėjo sistemoje. Be to, ji turėtų leisti informavimo apie sąskaitas paslaugų teikėjams ir mokėjimo inicijavimo paslaugų teikėjams pasikliauti autentiškumo patvirtinimo procedūromis, kurias sąskaitą tvarkantis mokėjimo paslaugų teikėjas nustato mokėjimo paslaugų vartotojui. Siekiant užtikrinti technologinį ir verslo modelio neutralumą, sąskaitas tvarkantys mokėjimo paslaugų teikėjai turėtų galėti savo nuožiūra nuspręsti, ar suteikti sąsają, specialiai skirtą ryšiams su informavimo apie sąskaitas paslaugų teikėjais, mokėjimo inicijavimo paslaugų teikėjais ir mokėjimo paslaugų teikėjais, išleidžiančiais kortele grindžiamas mokėjimo priemones, ar tiems ryšiams leisti naudoti sąsają, skirtą sąskaitas tvarkančių mokėjimo paslaugų teikėjų mokėjimo paslaugų vartotojams identifikuoti ir ryšiams su jais palaikyti;

(21) siekiant sudaryti sąlygas informavimo apie sąskaitas paslaugų teikėjams, mokėjimo inicijavimo paslaugų teikėjams ir mokėjimo paslaugų teikėjams, išleidžiantiems kortele grindžiamas mokėjimo priemones, kurti nuosavus techninius sprendimus, sąsajos techninės specifikacijos turėtų būti tinkamai dokumentuotos ir paviešintos. Be to, sąskaitą tvarkantis mokėjimo paslaugų teikėjas turėtų suteikti priemonę, kuria naudodamiesi mokėjimo paslaugų teikėjai galėtų testuoti techninius sprendimus bent šešis mėnesius iki šių reguliavimo standartų taikymo pradžios datos arba, jei šie sprendimai pradedami naudoti po šių standartų taikymo pradžios datos, iki datos, kurią sąsaja bus pateikta rinkai. Kad būtų užtikrintas skirtingų technologinių ryšių sprendimų sąveikumas, sąsaja turėtų būti grindžiama ryšių standartais, sukurtais tarptautinių arba Europos standartizacijos organizacijų;

(22) informavimo apie sąskaitas paslaugų teikėjų ir mokėjimo inicijavimo paslaugų teikėjų teikiamų paslaugų kokybė priklausys nuo tinkamo sąsajų, kurias įdiegė arba pritaikė sąskaitas tvarkantys mokėjimo paslaugų teikėjai, veikimo. Todėl tais atvejais, kai tokios sąsajos neatitinka šių standartų nuostatų, tokių paslaugų vartotojų labui svarbu imtis priemonių veiklos tęstinumui užtikrinti. Nacionalinės kompetentingos institucijos privalo užtikrinti, kad informavimo apie sąskaitas paslaugų teikėjams ir mokėjimo inicijavimo paslaugų teikėjams nebūtų užkertamas kelias ar trukdoma teikti savo paslaugų;

(23) kai prieiga prie mokėjimo sąskaitų yra teikiama naudojantis specialiąja sąsaja, siekiant užtikrinti mokėjimo paslaugų vartotojų teisę naudotis mokėjimo inicijavimo paslaugų teikėjų teikiamomis paslaugomis ir paslaugomis, kuriomis suteikiama prieiga prie sąskaitos informacijos, kaip numatyta Direktyvoje (ES) 2015/2366, būtina reikalauti užtikrinti, kad specialiosios sąsajos būtų tiek pat prieinamos ir tokios pat veiksmingos kaip mokėjimo paslaugų vartotojui prieinama sąsaja. Sąskaitas tvarkantys mokėjimo paslaugų teikėjai taip pat turėtų specialiųjų sąsajų prieinamumui ir veiksmingumui nustatyti skaidrius pagrindinius veiklos rodiklius ir paslaugų lygio tikslus, kurie būtų ne mažiau griežti nei nustatytieji jų mokėjimo paslaugų vartotojų naudojamai sąsajai. Tas sąsajas turėtų testuoti jas naudosiantys mokėjimo paslaugų teikėjai, o jų testavimą nepalankiausiomis sąlygomis ir stebėjimą turėtų atlikti kompetentingos institucijos;

(24) tam, kad mokėjimo paslaugų teikėjai, naudojantys specialiąją sąsają, galėtų toliau teikti savo paslaugas atvejais, kai sąsaja tampa neprieinama arba veikia netinkamai, būtina pagal griežtas sąlygas nustatyti atsarginį mechanizmą, leisiantį tokiems teikėjams naudoti sąsają, kurią sąskaitą tvarkantis mokėjimo paslaugų teikėjas naudoja savo mokėjimo paslaugų vartotojų identifikavimui ir ryšių su jais palaikymui. Tam tikri sąskaitas tvarkantys mokėjimo paslaugų teikėjai bus atleisti nuo pareigos pateikti tokį atsarginį mechanizmą, kadangi suteikia prieigą prie savo vartotojų sąsajų, jeigu jų kompetentingos institucijos nustato, kad specialiosios sąsajos atitinka konkrečias sąlygas, kuriomis užtikrinama netrukdoma konkurencija. Jeigu specialiosios sąsajos, kurioms taikoma išimtis, neatitinka privalomų sąlygų, atitinkamos kompetentingos institucijos suteiktas išimtis atšaukia;

(25) tam, kad sudarytų sąlygas kompetentingoms institucijoms veiksmingai prižiūrėti ir stebėti ryšių sąsajų diegimą ir valdymą, sąskaitas tvarkantys mokėjimo paslaugų teikėjai savo interneto svetainėse turėtų pateikti atitinkamų turimų dokumentų santrauką, o kritinių situacijų atveju gavę prašymą sprendimų dokumentaciją pateikti kompetentingoms institucijoms. Sąskaitas tvarkantys mokėjimo paslaugų teikėjai taip pat turėtų paviešinti tos sąsajos prieinamumo ir veiksmingumo statistinius duomenis;

(26) siekiant apsaugoti duomenų konfidencialumą ir vientisumą, būtina užtikrinti sąskaitas tvarkančių mokėjimo paslaugų teikėjų, informavimo apie sąskaitas paslaugų teikėjų, mokėjimo inicijavimo paslaugų teikėjų ir mokėjimo paslaugų teikėjų, išleidžiančių kortele grindžiamas mokėjimo priemones, ryšių seansų saugumą. Visų pirma

būtina įpareigoti sąskaitas tvarkančius mokėjimo paslaugų teikėjus, informavimo apie sąskaitas paslaugų teikėjus, mokėjimo inicijavimo paslaugų teikėjus ir mokėjimo paslaugų teikėjus, išleidžiančius kortele grindžiamas mokėjimo priemones, keičiantis duomenimis taikyti saugaus šifravimo technologijas;

(27) siekiant didinti vartotojų pasitikėjimą ir užtikrinti griežtą kliento autentiškumo patvirtinimą, reikėtų atsižvelgti į elektroninių atpažinties priemonių ir patikimumo užtikrinimo paslaugų, nustatytų Europos Parlamento ir Tarybos reglamentu (ES) Nr. 910/2014 ([1]), naudojimą, visų pirma paskelbtųjų elektroninės atpažinties schemų atžvilgiu;

(28) siekiant užtikrinti vienodą teisės aktų taikymo pradžios datą, šis reglamentas turėtų būti pradėtas taikyti tą pačią dieną, nuo kurios valstybės narės turi užtikrinti Direktyvos (ES) 2015/2366 65, 66, 67 ir 97 straipsniuose nurodytų saugumo priemonių taikymą;

(29) šis reglamentas grindžiamas Europos bankininkystės institucijos (EBI) Komisijai pateiktais techninių reguliavimo standartų projektais;

(30) EBI surengė atviras ir skaidrias viešas konsultacijas dėl techninių reguliavimo standartų projektų, kuriais grindžiamas šis reglamentas, išanalizavo galimas susijusias sąnaudas bei naudą ir paprašė Bankininkystės suinteresuotųjų subjektų grupės, įsteigtos pagal Reglamento (ES) Nr. 1093/2010 37 straipsnį, nuomonės,

PRIĖMĖ ŠĮ REGLAMENTĄ:

I SKYRIUS

BENDROSIOS NUOSTATOS

1 straipsnis

Dalykas

Šiuo reglamentu nustatomi reikalavimai, kurių turi laikytis mokėjimo paslaugų teikėjai, diegdami saugumo priemones, sudarysiančias jiems sąlygas atlikti šiuos veiksmus:

a) pagal Direktyvos (ES) 2015/2366 97 straipsnį taikyti griežto kliento autentiškumo patvirtinimo procedūrą;

b) netaikyti griežto kliento autentiškumo patvirtinimo saugumo reikalavimų, laikantis nurodytų ribojančių sąlygų, pagrįstų mokėjimo operacijos rizikos lygiu, suma, vykdymo pasikartojimo dažnumu ir mokėjimo kanalu;

c) apsaugoti mokėjimo paslaugų vartotojo personalizuotų saugumo požymių konfidencialumą ir vientisumą;

d) nustatyti sąskaitas tvarkančių mokėjimo paslaugų teikėjų, mokėjimo inicijavimo paslaugų teikėjų, informavimo apie sąskaitas paslaugų teikėjų, mokėtojų, gavėjų ir kitų mokėjimo paslaugų teikėjų bendrus ir saugius atviruosius ryšių standartus, taikytinus teikiant ir naudojant mokėjimo paslaugas įgyvendinant Direktyvos (ES) 2015/2366 IV antrąštinės dalies nuostatas.

2 straipsnis

Bendrieji autentiškumo patvirtinimo reikalavimai

1. Mokėjimo paslaugų teikėjai įdiegia operacijų stebėjimo mechanizmus, leidžiančius jiems aptikti neautorizuotas ar nesąžiningas mokėjimo operacijas, kad galėtų įgyvendinti saugumo priemones, nurodytas 1 straipsnio a ir b punktuose.

([1]) 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB (OL L 257, 2014 8 28, p. 53).

Tie mechanizmai yra grindžiami mokėjimo operacijų analize, kurią atliekant atsižvelgiama į mokėjimo paslaugų vartotojui būdingus elementus įprastu būdu naudojant personalizuotus saugumo požymius.

2. 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 prieigos prietaisą arba programinę įrangą suteikė mokėjimo paslaugų teikėjas, mokėjimo paslaugų vartotojui suteikto prieigos prietaiso arba programinės įrangos naudojimo ir netinkamo jų naudojimo žurnalą.

3 straipsnis

Saugumo priemonių peržiūra

1. 1 straipsnyje nurodytų saugumo priemonių įgyvendinimas dokumentuojamas, jos reguliariai testuojamos ir vertinamos, be to, jų auditą pagal mokėjimo paslaugų teikėjui taikytiną teisinę sistemą atlieka veiklos požiūriu nuo mokėjimo paslaugų teikėjo nepriklausomi ir jam nepavaldūs auditoriai, turintys IT saugumo ir mokėjimų srities kompetencijos.

2. Intervalai tarp 1 dalyje nurodytų auditų nustatomi atsižvelgiant į atitinkamą apskaitos ir teisės aktų nustatyto audito sistemą, taikytiną mokėjimo paslaugų teikėjui.

Tačiau 18 straipsnyje nurodytą išimtį taikančių mokėjimo paslaugų teikėjų atveju metodikos, modelio ir praneštų sukčiavimo rodiklių auditas vykdomas bent kas metus. Šį auditą atlieka veiklos požiūriu nuo mokėjimo paslaugų teikėjo nepriklausomas ir jam nepavaldus auditorius, turintis IT saugumo ir mokėjimų srities kompetencijos. Pirmaisiais 18 straipsnyje nurodytos išimties taikymo metais ir bent kas trejus metus vėliau arba dažniau, jei to prašo kompetentinga institucija, šį auditą atlieka nepriklausomas kvalifikuotas išorės auditorius.

3. Atliekant šį auditą pateikiamas įvertinimas ir ataskaita dėl mokėjimo paslaugų teikėjo saugumo priemonių atitikties šio reglamento reikalavimams.

Visa ataskaita paprašius pateikiama kompetentingoms institucijoms.

II SKYRIUS

GRIEŽTO KLIENTO AUTENTIŠKUMO PATVIRTINIMO TAIKYMO SAUGUMO PRIEMONĖS

4 straipsnis

Atpažinties kodas

1. Kai mokėjimo paslaugų teikėjai pagal Direktyvos (ES) 2015/2366 97 straipsnio 1 dalį taiko griežtą kliento autentiškumo patvirtinimą, autentiškumo patvirtinimas grindžiamas dviem ar daugiau žinojimo, turėjimo ir būdingumo kategorijų elementų, o jo rezultatas – sukurtas atpažinties kodas.

Mokėjimo paslaugų teikėjas priima atpažinties kodą tik vieną kartą, kai mokėtojas juo naudojasi internetu prisijungdamas prie savo mokėjimo sąskaitos, inicijuodamas elektroninę mokėjimo operaciją arba nuotolinio ryšio priemone vykdydamas bet kokį veiksmą, kuris gali būti susijęs su sukčiavimo atliekant mokėjimą ar kitokio piktnaudžiavimo rizika.

2. Taikant 1 dalį, mokėjimo paslaugų teikėjai priima saugumo priemones, kuriomis užtikrinama, kad būtų vykdomi visi šie reikalavimai:

a) atskleidus atpažinties kodą negali būti įmanoma sužinoti jokios informacijos apie 1 dalyje nurodytus elementus;

b) remiantis žiniomis apie bet kurį anksčiau sukurtą kitą atpažinties kodą, negali būti įmanoma sukurti naujo atpažinties kodo;

c) atpažinties kodo negali būti įmanoma suklastoti.

3. Mokėjimo paslaugų teikėjai užtikrina, kad autentiškumo patvirtinimas sukuriant atpažinties kodą apimtų kiekvieną iš šių priemonių:

a) kai autentiškumo patvirtinimui jungiantis nuotoliniu būdu, atliekant nuotolinius elektroninius mokėjimus arba vykdant nuotolinio ryšio priemone kitus veiksmus, kurie gali būti susiję su sukčiavimo atliekant mokėjimą ar kitokio piktnaudžiavimo rizika, nepavyksta sukurti atpažinties kodo 1 dalies tikslais, turi būti neįmanoma nustatyti, kuris iš toje dalyje nurodytų elementų buvo neteisingas;

b) iš eilės nepavykusių autentiškumo patvirtinimo mėginimų skaičius, kurį pasiekus Direktyvos (ES) 2015/2366 97 straipsnio 1 dalyje nurodyti veiksmai laikinai arba visam laikui užblokuojami, neviršija penkių per konkretų laikotarpį;

c) pagal V skyriaus reikalavimus ryšių seansai yra apsaugoti nuo autentiškumo patvirtinimo duomenų perėmimo autentiškumo patvirtinimo proceso metu ir nuo neturinčių leidimo asmenų manipuliavimo;

d) ilgiausias laikas, per kurį internetu prisijungęs prie savo mokėjimo sąskaitos mokėtojas neatlieka jokių veiksmų po autentiškumo patvirtinimo, neviršija penkių minučių.

4. Kai 3 dalies b punkte nurodytas užblokavimas yra laikinas, to užblokavimo trukmė ir bandymų skaičius yra nustatomi pagal mokėtojui teikiamos paslaugos savybes ir visų atitinkamų rūšių riziką, atsižvelgiant bent į 2 straipsnio 2 dalyje nurodytus veiksnius.

Prieš nustatant užblokavimą visam laikui, mokėtojas apie tai įspėjamas.

Nustačius užblokavimą visam laikui, nustatoma saugi procedūra, leidžianti mokėtojui atgauti užblokuotas elektronines mokėjimo priemones.

5 straipsnis

Dinamiškas susiejimas

1. Kai mokėjimo paslaugų teikėjai pagal Direktyvos (ES) 2015/2366 97 straipsnio 2 dalį taiko griežtą kliento autentiškumo patvirtinimą, be šio reglamento 4 straipsnio reikalavimų, jie priima ir saugumo priemones, atitinkančias visus šiuos reikalavimus:

a) mokėtojas informuojamas apie mokėjimo operacijos sumą ir gavėją;

b) sukurtas atpažinties kodas yra susietas su mokėjimo operacijos suma ir gavėju, kuriuos inicijuodamas operaciją patvirtina mokėtojas;

c) mokėjimo paslaugų teikėjo priimamas atpažinties kodas atitinka mokėjimo operacijos pirminę konkrečią sumą ir gavėjo tapatybę, kuriuos patvirtino mokėtojas;

d) dėl visų sumos arba gavėjo pakeitimų sukurtas atpažinties kodas tampa negaliojančiu.

2. Taikant 1 dalį, mokėjimo paslaugų teikėjai priima saugumo priemones, kuriomis užtikrinamas toliau išvardytų elementų konfidencialumas, autentiškumas ir vientisumas:

a) operacijos sumos ir gavėjo visais autentiškumo patvirtinimo etapais;

b) mokėtojui rodomos informacijos visais autentiškumo patvirtinimo etapais, įskaitant atpažinties kodo kūrimo, perdavimo ir naudojimo.

3. Taikant 1 dalies b punktą, kai mokėjimo paslaugų teikėjai pagal Direktyvos (ES) 2015/2366 97 straipsnio 2 dalį taiko griežtą kliento autentiškumo patvirtinimą, atpažinties kodui taikomi šie reikalavimai:

a) vykdant kortele grindžiamą mokėjimo operaciją, kai mokėtojas pagal tos direktyvos 75 straipsnio 1 dalį yra davęs sutikimą dėl tikslios lėšų sumos užblokavimo, atpažinties kodas yra susietas su suma, kurią mokėtojas davė sutikimą užblokuoti ir patvirtino inicijuodamas operaciją;

b) vykdant mokėjimo operacijas, kai mokėtojas yra davęs sutikimą įvykdyti keletą elektroninių nuotolinių mokėjimo vienam ar keliems gavėjams operacijų, atpažinties kodas yra susietas su bendra kelių mokėjimo operacijų suma ir nurodytais gavėjais.

6 straipsnis

Žinojimo kategorijos elementams taikomi reikalavimai

1. Mokėjimo paslaugų teikėjai priima priemones, kuriomis mažinama rizika, kad griežto kliento autentiškumo patvirtinimo elementus, priskiriamus prie žinojimo kategorijos, sužinos neturinčios leidimo šalys ar jie bus atskleisti neturinčioms leidimo šalims.

2. Siekdamas išvengti šių elementų atskleidimo neturinčioms leidimo šalims, naudodamasis šiais elementais mokėtojas taiko rizikos mažinimo priemones.

7 straipsnis

Turėjimo kategorijos elementams taikomi reikalavimai

1. Mokėjimo paslaugų teikėjai priima priemones, kuriomis mažinama rizika, kad griežto kliento autentiškumo patvirtinimo elementais, priskiriamais prie turėjimo kategorijos, pasinaudos neturinčios leidimo šalys.

2. Naudodamasis šiais elementais mokėtojas taiko priemones, kuriomis siekiama išvengti šių elementų kopijavimo.

8 straipsnis

Su būdingumo kategorijos elementais susijusiems prietaisams ir programinei įrangai taikomi reikalavimai

1. Mokėjimo paslaugų teikėjai priima priemones, kuriomis mažinama rizika, kad griežto kliento autentiškumo patvirtinimo elementus, priskiriamus prie būdingumo kategorijos ir nuskaitomus mokėtojui pateiktais prieigos prietaisais ir programine įranga, sužinos neturinčios leidimo šalys. Mokėjimo paslaugų teikėjai bent užtikrina, kad tikimybė naudojantis tais prieigos prietaisais ir programine įranga mokėtoju patvirtinti neturinčią leidimo šalį būtų labai maža.

2. Naudodamasis šiais elementais mokėtojas taiko priemones, kuriomis užtikrinama, kad tie prietaisai ir programinė įranga garantuotų apsaugą nuo neautorizuoto elementų naudojimo prisijungus prie prietaisų ir programinės įrangos.

9 straipsnis

Elementų nepriklausomumas

1. Mokėjimo paslaugų teikėjai užtikrina, kad griežto kliento autentiškumo patvirtinimo elementų naudojimui pagal 6, 7 ir 8 straipsnius būtų taikomos priemonės, kuriomis užtikrinama, kad technologijų, algoritmų ir parametrų požiūriais pažeidus vieną elementą nebūtų paveiktas kitų patikimumas.

2. Mokėjimo paslaugų teikėjai priima saugumo priemones, kuriomis tais atvejais, kai kuris nors griežto kliento autentiškumo patvirtinimo elementas arba pats atpažinties kodas naudojamas universaliame prietaise, mažinama rizika, kuri galėtų kilti, jei to universalaus prietaiso patikimumas būtų paveiktas.

3. Taikant 2 dalį, rizikos mažinimo priemonės apima visus šiuos elementus:

a) atskirų saugių vykdymo aplinkų naudojimą įdiegus programinę įrangą universaliame prietaise;

b) mechanizmus, kuriais užtikrinama, kad mokėtojas ar trečioji šalis negalėtų pakeisti nei programinės įrangos, nei prietaiso;

c) įvykus pakeitimams – jų padarinius mažinančius mechanizmus.

III SKYRIUS

GRIEŽTO KLIENTO AUTENTIŠKUMO PATVIRTINIMO IŠIMTYS

10 straipsnis

Mokėjimo sąskaitos informacija

1. Mokėjimo paslaugų teikėjams leidžiama netaikyti griežto kliento autentiškumo patvirtinimo, jeigu jie įvykdo 2 straipsnio ir šio straipsnio 2 dalies reikalavimus ir kai mokėjimo paslaugų vartotojas, neatskleisdamas neskelbtinų mokėjimo duomenų, turi ribotą galimybę internetu sužinoti vieną ar abu šiuos dalykus:

a) vienos ar kelių nurodytų mokėjimo sąskaitų likutį;

b) per paskutines 90 dienų naudojantis viena ar keliomis nurodytomis mokėjimo sąskaitomis įvykdytas mokėjimo operacijas.

2. Taikant 1 dalį, mokėjimo paslaugų teikėjams griežto kliento autentiškumo patvirtinimo taikymo išimtis nėra taikoma, kai įvykdoma kuri nors iš šių sąlygų:

a) mokėjimo paslaugų vartotojas internetu susipažįsta su 1 dalyje nurodyta informacija pirmą kartą;

b) praėjo daugiau kaip 90 dienų nuo tada, kai mokėjimo paslaugų vartotojas paskutinį kartą internetu susipažino su 1 dalies b punkte nurodyta informacija ir buvo taikytas griežtas kliento autentiškumo patvirtinimas.

11 straipsnis

Bekontakčiai mokėjimai pardavimo vietose

Mokėjimo paslaugų teikėjams leidžiama netaikyti griežto kliento autentiškumo patvirtinimo, jeigu jie įvykdo 2 straipsnio reikalavimus, kai mokėtojas inicijuoja bekontaktę elektroninę mokėjimo operaciją, su sąlyga, kad įvykdomos šios sąlygos:

a) atskiros bekontaktės elektroninės mokėjimo operacijos vertė neviršija 50 EUR ir

b) bendra ankstesnių bekontakčių elektroninių mokėjimo operacijų, inicijuotų mokėjimo priemone, turinčia bekontaktę funkciją, vertė nuo paskutinio karto, kai taikytas griežtas kliento autentiškumo patvirtinimas, neviršija 150 EUR arba

c) iš eilės vykdytų bekontakčių elektroninių mokėjimo operacijų, inicijuotų mokėjimo priemone, turinčia bekontaktę funkciją, skaičius nuo paskutinio karto, kai taikytas griežtas kliento autentiškumo patvirtinimas, neviršija penkių.

12 straipsnis

Neprižiūrimi transporto ir automobilių stovėjimo mokesčių terminalai

Mokėjimo paslaugų teikėjams leidžiama netaikyti griežto kliento autentiškumo patvirtinimo, jeigu jie įvykdo 2 straipsnio reikalavimus, kai mokėtojas inicijuoja elektroninę mokėjimo operaciją neprižiūrimame mokėjimo terminale siekdamas sumokėti transporto ar automobilių stovėjimo mokesčius.

13 straipsnis

Patikimi gavėjai

1. Mokėjimo paslaugų teikėjai taiko griežtą kliento autentiškumo patvirtinimą, kai mokėtojas kuria ar keičia patikimų gavėjų sąrašą mokėtojo sąskaitą tvarkančio mokėjimo paslaugų teikėjo sistemoje.

2. Mokėjimo paslaugų teikėjams leidžiama netaikyti griežto kliento autentiškumo patvirtinimo, jeigu jie įvykdo bendruosius autentiškumo patvirtinimo reikalavimus, kai mokėtojas inicijuoja mokėjimo operaciją ir gavėjas jau yra anksčiau mokėtojo sukurtame patikimų gavėjų sąraše.

14 straipsnis

Pasikartojančios operacijos

1. Mokėjimo paslaugų teikėjai taiko griežtą kliento autentiškumo patvirtinimą, kai mokėtojas kuria, keičia ar pirmą kartą inicijuoja pasikartojančias operacijas, kurių suma yra vienoda, o gavėjas tas pats.

2. Mokėjimo paslaugų teikėjams leidžiama netaikyti griežto kliento autentiškumo patvirtinimo, jeigu jie įvykdo bendruosius autentiškumo patvirtinimo reikalavimus, kai inicijuojamos visos paskesnės mokėjimo operacijos, priklausančios 1 dalyje nurodytoms pasikartojančioms operacijoms.

15 straipsnis

Kredito pervedimai tarp to paties fizinio ar juridinio asmens sąskaitų

Mokėjimo paslaugų teikėjams leidžiama netaikyti griežto kliento autentiškumo patvirtinimo, jeigu jie įvykdo 2 straipsnio reikalavimus, kai mokėtojas inicijuoja kredito pervedimą tais atvejais, kai mokėtojas ir gavėjas yra tas pats fizinis arba juridinis asmuo ir abi mokėjimo sąskaitas tvarko tas pats sąskaitą tvarkantis mokėjimo paslaugų teikėjas.

16 straipsnis

Mažos vertės operacijos

Mokėjimo paslaugų teikėjams leidžiama netaikyti griežto kliento autentiškumo patvirtinimo, kai mokėtojas inicijuoja nuotolinę elektroninę mokėjimo operaciją, jeigu įvykdomos šios sąlygos:

a) nuotolinės elektroninės mokėjimo operacijos vertė neviršija 30 EUR ir

b) ankstesnių nuotolinių elektroninių mokėjimo operacijų, mokėtojo inicijuotų nuo paskutinio karto, kai taikytas griežtas kliento autentiškumo patvirtinimas, bendra vertė neviršija 100 EUR arba

c) ankstesnių nuotolinių elektroninių mokėjimo operacijų, mokėtojo inicijuotų nuo paskutinio karto, kai taikytas griežtas kliento autentiškumo patvirtinimas, skaičius neviršija penkių atskirų nuotolinių elektroninių mokėjimo operacijų iš eilės.

17 straipsnis

Saugūs įmonių mokėjimo procesai ir protokolai

Mokėjimo paslaugų teikėjams leidžiama netaikyti griežto kliento autentiškumo patvirtinimo juridiniams asmenims, inicijuojantiems elektronines mokėjimo operacijas naudojant specialius mokėjimo procesus ar protokolus, prieinamus tik mokėtojams, kurie nėra vartotojai, kai kompetentingos institucijos įsitikina, kad tais procesais ar protokolais užtikrinamo saugumo lygis yra ne žemesnis nei numatytasis Direktyvoje (ES) 2015/2366.

18 straipsnis

Operacijos rizikos analizė

1. Mokėjimo paslaugų teikėjams leidžiama netaikyti griežto kliento autentiškumo patvirtinimo, kai mokėtojas inicijuoja nuotolinę elektroninę mokėjimo operaciją, kuri, mokėjimo paslaugų teikėjo vertinimu, yra mažai rizikinga pagal operacijų stebėjimo mechanizmus, nurodytus 2 straipsnyje ir šio straipsnio 2 dalies c punkte.

2. 1 dalyje nurodyta elektroninė mokėjimo operacija laikoma mažai rizikinga, kai įvykdomos visos šios sąlygos:

a) mokėjimo paslaugų teikėjo nurodytas ir pagal 19 straipsnį apskaičiuotas šios rūšies operacijų sukčiavimo rodiklis prilygsta orientaciniams sukčiavimo rodikliams, nurodytiems priedo lentelėje atitinkamai prie „nuotolinių elektroninių kortele grindžiamų mokėjimų“ ir „nuotolinių elektroninių kredito pervedimų“, arba yra už juos mažesnis;

b) operacijos suma neviršija atitinkamos išimties ribinės vertės, nurodytos priedo lentelėje;

c) atlikdami rizikos analizę realiuoju laiku mokėjimo paslaugų teikėjai nenustatė nė vieno iš šių:

   i) mokėtojui nebūdingų išlaidų arba elgsenos modelių;

   ii) neįprastos informacijos apie mokėtojo prieigą naudojantis prietaisu ir (arba) programine įranga;

   iii) užkrėtimo kenkimo programine įranga per bet kurį autentiškumo patvirtinimo seansą;

   iv) žinomo sukčiavimo scenarijaus teikiant mokėjimo paslaugas;

   v) mokėtojui nebūdingos buvimo vietos;

   vi) labai rizikingos gavėjo buvimo vietos.

3. Mokėjimo paslaugų teikėjai, ketinantys netaikyti griežto kliento autentiškumo patvirtinimo elektroninėms nuotolinėms mokėjimo operacijoms, nes šios yra mažos rizikos, atsižvelgia bent į šiuos rizika grindžiamus veiksnius:

a) ankstesnius atskiro mokėjimo paslaugų vartotojo išlaidų modelius;

b) ankstesnes kiekvieno mokėjimo paslaugų teikėjo mokėjimo paslaugų vartotojo mokėjimų operacijas;

c) mokėtojo ir gavėjo vietą mokėjimo operacijos vykdymo metu tais atvejais, kai prieigos prietaisą arba programinę įrangą suteikė mokėjimo paslaugų teikėjas;

d) nustatytus mokėjimo paslaugų vartotojui nebūdingus mokėjimo modelius, lyginant su ankstesnėmis šio vartotojo mokėjimo operacijomis.

Siekdamas nustatyti, ar konkrečiam mokėjimui galima netaikyti griežto kliento autentiškumo patvirtinimo, mokėjimo paslaugų teikėjas atlikdamas vertinimą visus šiuos rizika grindžiamus veiksnius įtraukia į kiekvienos atskiros operacijos rizikos įvertinimą.

19 straipsnis

Sukčiavimo rodiklių apskaičiavimas

1. Mokėjimo paslaugų teikėjas užtikrina, kad kiekvienos priedo lentelėje nurodytos rūšies operacijų bendri sukčiavimo rodikliai, apimantys tiek mokėjimo operacijas, kurių autentiškumas patvirtintas taikant griežtą kliento autentiškumo patvirtinimą, tiek pagal 13–18 straipsniuose nurodytas išimtis įvykdytas mokėjimo operacijas, prilygsta tos pačios priedo lentelėje nurodytos rūšies operacijų orientaciniams sukčiavimo rodikliams arba yra už juos mažesni.

Kiekvienos rūšies operacijų bendri sukčiavimo rodikliai apskaičiuojami bendrą neautorizuotų arba nesąžiningų nuotolinių mokėjimo operacijų vertę, nepriklausomai nuo to, ar lėšos buvo atgautos, ar ne, padalijus iš visų tos pačios rūšies operacijų, kurių autentiškumas patvirtintas taikant griežtą kliento autentiškumo patvirtinimą arba kurios įvykdytos taikant bet kurią 13–18 straipsniuose nurodytą išimtį, bendros paskutinio ketvirčio (90 dienų) vertės.

2. Sukčiavimo rodiklių apskaičiavimo metodas ir gauti įverčiai patikrinami atliekant 3 straipsnio 2 dalyje nurodytą auditą, kuriuo užtikrinama, kad įverčiai būtų galutiniai ir tikslūs.

3. Mokėjimo paslaugų teikėjo naudojama metodika ir visi modeliai sukčiavimo rodikliams apskaičiuoti, taip pat patys sukčiavimo rodikliai yra tinkamai dokumentuojami ir visiškai atskleidžiami kompetentingoms institucijoms ir EBI, pateikus atitinkamai (-oms) kompetentingai (-oms) institucijai (-oms) išankstinį pranešimą, jei ji (jos) to prašo.

20 straipsnis

Remiantis operacijos rizikos analize atšauktos išimtys

1. Mokėjimo paslaugų teikėjai, kurie naudojasi 18 straipsnyje nurodyta išimtimi, nedelsdami kompetentingoms institucijoms praneša, jei kuris nors iš bet kurios rūšies mokėjimo operacijų, nurodytų priedo lentelėje, stebimų sukčiavimo rodiklių viršytų orientacinį sukčiavimo rodiklį, ir pateikia priemonių, kurias ketina priimti siekdami atkurti stebimų sukčiavimo rodiklių atitiktį taikytiniems orientaciniams sukčiavimo rodikliams, aprašymą.

2. Mokėjimo paslaugų teikėjai nedelsdami nustoja taikyti 18 straipsnyje nurodytą išimtį visų rūšių mokėjimo operacijoms, nurodytoms priedo lentelėje ir patenkančioms į konkretų išimties ribų intervalą, kai jų stebimas sukčiavimo rodiklis du ketvirčius iš eilės viršija orientacinį sukčiavimo rodiklį, taikytiną tai mokėjimo priemonei arba tos rūšies mokėjimo operacijoms tame išimties ribų intervale.

3. Pagal šio straipsnio 2 dalį nustoję taikyti 18 straipsnyje nurodytą išimtį, mokėjimo paslaugų teikėjai nepradeda ta išimtimi iš naujo naudotis tol, kol jų apskaičiuotas vieno ketvirčio sukčiavimo rodiklis neprilygsta tos rūšies mokėjimo operacijų, patenkančių į tą išimties ribų intervalą, orientaciniams sukčiavimo rodikliams arba nėra už juos mažesnis.

4. Kai mokėjimo paslaugų teikėjai ketina pradėti iš naujo taikyti 18 straipsnyje nurodytą išimtį, jie pakankamai iš anksto apie tai informuoja kompetentingas institucijas ir, prieš pradėdami vėl taikyti išimtį, pateikia įrodymus, kad pagal šio straipsnio 3 dalį jų stebimas sukčiavimo rodiklis vėl atitinka taikytiną orientacinį sukčiavimo rodiklį tame išimties ribų intervale.

21 straipsnis

Stebėjimas

1. Siekdami pasinaudoti 10–18 straipsniuose nurodytomis išimtimis, mokėjimo paslaugų teikėjai bent kas ketvirtį fiksuoja ir stebi šiuos kiekvienos rūšies mokėjimo operacijų, skirstomų į nuotolines ir nenuotolines mokėjimo operacijas, duomenis:

a) bendrą neautorizuotų ar nesąžiningų mokėjimo operacijų vertę pagal Direktyvos (ES) 2015/2366 64 straipsnio 2 dalį, bendrą visų mokėjimo operacijų vertę ir apskaičiuotą sukčiavimo rodiklį, taip pat suskirstant mokėjimo operacijas į inicijuotas taikant griežtą kliento autentiškumo patvirtinimą ir pagal kiekvieną iš išimčių;

b) vidutinę operacijos vertę, taip pat suskirstant mokėjimo operacijas į inicijuotas taikant griežtą kliento autentiškumo patvirtinimą ir pagal kiekvieną iš išimčių;

c) mokėjimo operacijų skaičių kiekvienos išimties taikymo atveju ir jų procentinę dalį, palyginti su bendru mokėjimo operacijų skaičiumi.

2. Stebėjimo pagal 1 dalį rezultatus mokėjimo paslaugų teikėjai pateikia kompetentingoms institucijoms ir EBI, o gavę prašymą atitinkamai (-oms) kompetentingai (-oms) institucijai (-oms) pateikia išankstinį pranešimą.

IV SKYRIUS

MOKĖJIMO PASLAUGŲ VARTOTOJŲ PERSONALIZUOTŲ SAUGUMO POŽYMIŲ KONFIDENCIALUMAS IR VIENTISUMAS

22 straipsnis

Bendrieji reikalavimai

1. Visais autentiškumo patvirtinimo etapais mokėjimo paslaugų teikėjai užtikrina mokėjimo paslaugų vartotojų personalizuotų saugumo požymių konfidencialumą ir vientisumą, pavyzdžiui, naudodami atpažinties kodus.

2. Taikydami 1 dalį, mokėjimo paslaugų teikėjai užtikrina, kad būtų vykdomi visi šie reikalavimai:

a) rodomi personalizuoti saugumo požymiai yra paslepiami ir negali būti visi perskaitomi, kai mokėjimo paslaugų vartotojas juos įveda autentiškumo patvirtinimo metu;

b) nei personalizuoti saugumo požymiai duomenų formatu, nei kriptografinė medžiaga, susijusi su personalizuotų saugumo požymių šifravimu, nesaugomi grynojo teksto (angl. *plaintext*) formatu;

c) slapta kriptografinė medžiaga apsaugoma nuo neteisėto atskleidimo.

3. Mokėjimo paslaugų teikėjai išsamiai dokumentuoja su kriptografinės medžiagos, naudojamos personalizuotų saugumo požymių šifravimui ar kitokiam jų nuskaitymo galimybės panaikinimui, valdymu susijusį procesą.

4. Mokėjimo paslaugų teikėjai užtikrina, kad personalizuotų saugumo požymių ir atpažinties kodų, sukurtų pagal II skyrių, tvarkymas ir nukreipimas vyktų saugioje aplinkoje laikantis griežtų visuotinai pripažintų sektoriaus standartų.

23 straipsnis

Požymių kūrimas ir perdavimas

Mokėjimo paslaugų teikėjai užtikrina, kad personalizuoti saugumo požymiai būtų kuriami saugioje aplinkoje.

Jie sumažina personalizuotų saugumo požymių ir atpažinties prietaisų bei programinės įrangos neautorizuoto naudojimo riziką po jų praradimo, vagystės ar nukopijavimo iki jų pateikimo mokėtojui.

24 straipsnis

Susiejimas su mokėjimo paslaugų vartotoju

1. Mokėjimo paslaugų teikėjai užtikrina, kad su personalizuotais saugumo požymiais ir atpažinties prietaisais bei programine įranga saugiu būdu būtų susietas tik mokėjimo paslaugų vartotojas.

2. Taikydami 1 dalį, mokėjimo paslaugų teikėjai užtikrina, kad būtų vykdomi visi šie reikalavimai:

a) personalizuotų saugumo požymių ir atpažinties prietaisų bei programinės įrangos susiejimas su mokėjimo paslaugų vartotojo tapatybe atliekamas saugioje aplinkoje, už kurią atsako mokėjimo paslaugų teikėjas ir kurią sudaro bent mokėjimo paslaugų teikėjo patalpos, mokėjimo paslaugų teikėjo suteikta interneto aplinka ar kitos panašios saugios interneto svetainės, kurias naudoja mokėjimo paslaugų teikėjas ir jo bankomatai, atsižvelgiant į riziką, susijusią su prietaisais ir pagrindiniais susiejimo procese naudojamais komponentais, už kuriuos mokėjimo paslaugų teikėjas neatsako;

b) personalizuotų saugumo požymių ir atpažinties prietaisų bei programinės įrangos susiejimas su mokėjimo paslaugų vartotojo tapatybe nuotolinio ryšio priemone atliekamas taikant griežtą kliento autentiškumo patvirtinimą.

25 straipsnis

Požymių, atpažinties prietaisų ir programinės įrangos pateikimas

1. Mokėjimo paslaugų teikėjai užtikrina, kad personalizuoti saugumo požymiai, atpažinties prietaisai ir programinė įranga mokėjimo paslaugų vartotojui būtų pateikti saugiu būdu, kuriuo užkertamas kelias jų neautorizuoto naudojimo dėl praradimo, vagystės ar nukopijavimo rizikai.

2. Taikydami 1 dalį, mokėjimo paslaugų teikėjai bent taiko visas šias priemones:

a) veiksmingas ir saugias pateikimo priemones, kuriomis užtikrinama, kad personalizuoti saugumo požymiai, atpažinties prietaisai ir programinė įranga būtų pateikti teisėtam mokėjimo paslaugų vartotojui;

b) priemones, leidžiančias mokėjimo paslaugų teikėjui patikrinti mokėjimo paslaugų vartotojui internetu pateiktos atpažinties programinės įrangos autentiškumą;

c) priemones, kuriomis užtikrinama, kad pateikiant personalizuotus saugumo požymius ne mokėjimo paslaugų teikėjo patalpose arba nuotolinio ryšio priemone:

   i) jokia neturinti leidimo šalis negalėtų gauti daugiau kaip vieno personalizuotų saugumo požymių, atpažinties prietaisų ir programinės įrangos elemento, kai šie pateikiami ta pačia ryšio priemone;

   ii) prieš naudojant pateiktus personalizuotus saugumo požymius, atpažinties prietaisus ir programinę įrangą, juos reikėtų aktyvinti;

d) priemones, kuriomis užtikrinama, kad tais atvejais, kai personalizuotus saugumo požymius, atpažinties prietaisus ir programinę įrangą reikia aktyvinti prieš pirmą jų panaudojimą, aktyvacija vyktų saugioje aplinkoje pagal 24 straipsnyje nurodytas susiejimo procedūras.

26 straipsnis

Personalizuotų saugumo požymių atnaujinimas

Mokėjimo paslaugų teikėjai užtikrina, kad personalizuotų saugumo požymių atnaujinimas arba pakartotinė aktyvacija vyktų laikantis požymių ir atpažinties prietaisų kūrimo, susiejimo ir pateikimo procedūrų pagal 23, 24 ir 25 straipsnius.

27 straipsnis

Sunaikinimas, deaktyvacija ir atšaukimas

Mokėjimo paslaugų teikėjai užtikrina veiksmingų procesų įdiegimą, kad būtų galima taikyti kiekvieną iš šių saugumo priemonių:

a) saugų personalizuotų saugumo požymių, atpažinties prietaisų ir programinės įrangos sunaikinimą, deaktyvaciją ar atšaukimą;

b) tais atvejais, kai mokėjimo paslaugų teikėjas platina pakartotinai naudojamus prietaisus ir programinę įrangą, – saugaus pakartotinio prietaiso arba programinės įrangos naudojimo nustatymą, dokumentavimą ir įgyvendinimą prieš pateikiant juos kitam mokėjimo paslaugų vartotojui;

c) informacijos, susijusios su personalizuotais saugumo požymiais ir saugomos mokėjimo paslaugų teikėjo sistemose ir duomenų bazėse, o atitinkamais atvejais ir viešose duomenų saugyklose, deaktyvaciją ar atšaukimą.

V SKYRIUS

BENDRI IR SAUGŪS ATVIRIEJI RYŠIŲ STANDARTAI

1 skirsnis

Ryšiams taikomi bendrieji reikalavimai

28 straipsnis

Identifikavimo reikalavimai

1. Mokėjimo paslaugų teikėjai užtikrina saugų identifikavimą atliekant elektroninius mokėjimus, kai užmezgamas ryšys tarp mokėtojo prietaiso ir gavėjo priėmimo prietaiso, įskaitant, be kita ko, mokėjimo terminalus.

2. Mokėjimo paslaugų teikėjai užtikrina, kad veiksmingai būtų sumažinta rizika, kad perduodami duomenys bus nukreipti neturinčioms leidimo šalims naudojant mobiliąsias programas ir kitas mokėjimo paslaugų vartotojų sąsajas, kuriomis teikiamos elektroninių mokėjimų paslaugos.

29 straipsnis

Atsekamumas

1. Mokėjimo paslaugų teikėjai įdiegia procesus, kuriais užtikrinama, kad visos mokėjimo operacijos ir kitų rūšių sąveika su mokėjimo paslaugų vartotoju, kitais mokėjimo paslaugų teikėjais ir kitais subjektais, įskaitant pardavėjus, teikiant mokėjimo paslaugą būtų atsekamos, kad vėliau būtų galima sužinoti apie visus su elektronine operacija įvairiais jos etapais susijusius įvykius.

2. Taikant 1 dalį, mokėjimo paslaugų teikėjai užtikrina, kad visiems ryšių seansams su mokėjimo paslaugų vartotoju, kitais mokėjimo paslaugų teikėjais ir kitais subjektais, įskaitant pardavėjus, būtų taikoma kiekviena iš šių priemonių:

a) seanso unikalus identifikatorius;

b) saugumo mechanizmai, įrašantys išsamius operacijos duomenis, įskaitant operacijos numerį, laiko žymas ir visus svarbius operacijos duomenis;

c) laiko žymos, grindžiamos bendrąja laiko nuorodų sistema ir sinchronizuojamos pagal oficialų laiko signalą.

2 skirsnis

Bendriems ir saugiems atviriesiems ryšių standartams taikomi konkretūs reikalavimai

30 straipsnis

Prieigos sąsajoms taikomi bendrieji reikalavimai

1. Sąskaitas tvarkantys mokėjimo paslaugų teikėjai, suteikiantys mokėtojui mokėjimo sąskaitą, kuri yra prieinama internetu, įdiegia bent vieną sąsają, atitinkančią kiekvieną iš šių reikalavimų:

a) informavimo apie sąskaitas paslaugų teikėjai, mokėjimo inicijavimo paslaugų teikėjai ir mokėjimo paslaugų teikėjai, išleidžiantys kortele grindžiamas mokėjimo priemones, gali identifikuotis sąskaitą tvarkančio mokėjimo paslaugų teikėjo sistemoje;

b) informavimo apie sąskaitas paslaugų teikėjai gali palaikyti saugius ryšius prašydami informacijos apie vieną ar daugiau nurodytų mokėjimo sąskaitų ir susijusias mokėjimo operacijas ir šią informaciją gaudami;

c) mokėjimo inicijavimo paslaugų teikėjai gali palaikyti saugius ryšius inicijuodami mokėjimo nurodymo vykdymą iš mokėtojo mokėjimo sąskaitos ir gaudami visą informaciją apie mokėjimo operacijos inicijavimą ir visą informaciją, prieinamą sąskaitas tvarkantiems mokėjimo paslaugų teikėjams, apie mokėjimo operacijos įvykdymą.

2. Mokėjimo paslaugų vartotojo autentiškumo patvirtinimo tikslu 1 dalyje nurodyta sąsaja turėtų leisti informavimo apie sąskaitas paslaugų teikėjams ir mokėjimo inicijavimo paslaugų teikėjams pasikliauti visomis autentiškumo patvirtinimo procedūromis, kurias sąskaitą tvarkantis mokėjimo paslaugų teikėjas nustato mokėjimo paslaugų vartotojui.

Sąsaja turi atitikti bent visus šiuos reikalavimus:

a) mokėjimo inicijavimo paslaugų teikėjas arba informavimo apie sąskaitas paslaugų teikėjas turi galėti nurodyti sąskaitą tvarkančiam mokėjimo paslaugų teikėjui pradėti autentiškumo patvirtinimą, remiantis mokėjimo paslaugų vartotojo sutikimu;

b) sąskaitas tvarkančių mokėjimo paslaugų teikėjų, informavimo apie sąskaitas paslaugų teikėjų, mokėjimo inicijavimo paslaugų teikėjų ir visų susijusių mokėjimo paslaugų vartotojų ryšių seansai pradedami ir palaikomi visą autentiškumo patvirtinimo procesą;

c) užtikrinamas personalizuotų saugumo požymių ir atpažinties kodų, perduodamų mokėjimo inicijavimo paslaugų teikėjo arba informavimo apie sąskaitas paslaugų teikėjo arba per juos, vientisumas ir konfidencialumas.

3. Sąskaitas tvarkantys mokėjimo paslaugų teikėjai užtikrina, kad jų sąsajos atitiktų ryšių standartus, paskelbtus tarptautinių arba Europos standartizacijos organizacijų.

Sąskaitas tvarkantys mokėjimo paslaugų teikėjai taip pat užtikrina, kad visų sąsajų techninės specifikacijos būtų dokumentuotos, nurodant procedūras, protokolus ir priemones, reikalingus mokėjimo inicijavimo paslaugų teikėjams, informavimo apie sąskaitas paslaugų teikėjams ir mokėjimo paslaugų teikėjams, išleidžiantiems kortele grindžiamas mokėjimo priemones, kad jų programinė įranga ir programos galėtų sąveikauti su sąskaitas tvarkančių mokėjimo paslaugų teikėjų sistemomis.

Ne vėliau kaip likus šešiems mėnesiams iki 38 straipsnio 2 dalyje nurodytos taikymo pradžios datos arba iki numatytos prieigos sąsajos pateikimo rinkai datos, kai ji yra po 38 straipsnio 2 dalyje nurodytos datos, sąskaitas tvarkantys mokėjimo paslaugų teikėjai nemokamai paprašius pateikia bent turimus dokumentus turintiems leidimą mokėjimo inicijavimo paslaugų teikėjams, informavimo apie sąskaitas paslaugų teikėjams ir mokėjimo paslaugų teikėjams, išleidžiantiems kortele grindžiamas mokėjimo priemones, arba mokėjimo paslaugų teikėjams, kurie į savo kompetentingas institucijas kreipėsi dėl atitinkamo leidimo, ir savo interneto svetainėje paviešina dokumentų santrauką.

4. Be 3 dalies taikymo, sąskaitas tvarkantys mokėjimo paslaugų teikėjai užtikrina, kad, išskyrus kritinės situacijos atvejus, apie visus jų sąsajos techninių specifikacijų pakeitimus iš anksto, kai tik tampa įmanoma, bet ne vėliau kaip likus 3 mėnesiams iki pakeitimo įdiegimo, būtų pranešta leidimus turintiems mokėjimo inicijavimo paslaugų teikėjams, informavimo apie sąskaitas paslaugų teikėjams ir mokėjimo paslaugų teikėjams, išleidžiantiems kortele grindžiamas mokėjimo priemones, arba mokėjimo paslaugų teikėjams, kurie į savo kompetentingas institucijas kreipėsi dėl atitinkamo leidimo.

Mokėjimo paslaugų teikėjai dokumentuoja kritines situacijas, kurioms susiklosčius buvo atlikti pakeitimai, ir paprašius pateikia dokumentus kompetentingoms institucijoms.

5. Sąskaitas tvarkantys mokėjimo paslaugų teikėjai suteikia prisijungimo ir funkcinio išbandymo testavimo priemonę, įskaitant pagalbą, leidimus turintiems mokėjimo inicijavimo paslaugų teikėjams, informavimo apie sąskaitas paslaugų teikėjams ir mokėjimo paslaugų teikėjams, išleidžiantiems kortele grindžiamas mokėjimo priemones, arba mokėjimo paslaugų teikėjams, kurie į savo kompetentingas institucijas kreipėsi dėl atitinkamo leidimo, kad šie testuotų savo programinę įrangą ir programas, naudojamas mokėjimo paslaugoms vartotojams teikti. Ši testavimo priemonė turėtų būti pateikta ne vėliau kaip likus šešiems mėnesiams iki 38 straipsnio 2 dalyje nurodytos taikymo pradžios datos arba iki numatytos prieigos sąsajos pateikimo rinkai datos, kai ji yra po 38 straipsnio 2 dalyje nurodytos datos.

Tačiau naudojantis testavimo priemone negali būti dalijamasi jokia neskelbtina informacija.

6. Kompetentingos institucijos užtikrina, kad sąskaitas tvarkantys mokėjimo paslaugų teikėjai visą laiką laikytųsi šiuose standartuose nurodytų pareigų, susijusių su jų įdiegtomis sąsajomis. Jeigu sąskaitą tvarkantis mokėjimo paslaugų teikėjas nesilaiko šiuose standartuose sąsajoms nustatytų reikalavimų, kompetentingos institucijos užtikrina, kad mokėjimo inicijavimo paslaugų ir informavimo apie sąskaitas paslaugų teikimui nebūtų kliudoma ir jis nebūtų trikdomas, jeigu atitinkami tų paslaugų teikėjai laikosi 33 straipsnio 5 dalyje nurodytų sąlygų.

31 straipsnis

Galimos prieigos sąsajos

Sąskaitas tvarkantys mokėjimo paslaugų teikėjai pateikia 30 straipsnyje nurodytą (-as) sąsają (-as) įdiegdami specialiąją sąsają arba leisdami 30 straipsnio 1 dalyje nurodytiems mokėjimo paslaugų teikėjams naudoti sąsajas, naudojamas autentiškumo patvirtinimui ir ryšiams su sąskaitą tvarkančio mokėjimo paslaugų teikėjo mokėjimo paslaugų vartotojais.

32 straipsnis

Specialiajai sąsajai taikomi reikalavimai

1. Laikantis 30 ir 31 straipsnių, specialiąją sąsają įdiegę sąskaitas tvarkantys mokėjimo paslaugų teikėjai užtikrina, kad specialioji sąsaja visą laiką būtų tiek pat prieinama ir tokia pati veiksminga, įskaitant pagalbą, kaip sąsajos, kuriomis mokėjimo paslaugų vartotojas gali tiesiogiai internetu jungtis prie savo mokėjimo sąskaitos.

2. Specialiąją sąsają įdiegę sąskaitas tvarkantys mokėjimo paslaugų teikėjai nustato skaidrius pagrindinius veiklos rodiklius ir paslaugų lygio tikslus, kurie prieinamumo ir pagal 36 straipsnį teikiamų duomenų požiūriais būtų ne mažiau griežti nei nustatytieji jų mokėjimo paslaugų vartotojų naudojamai sąsajai. Šių sąsajų, rodiklių ir tikslų stebėjimą ir testavimą nepalankiausiomis sąlygomis atlieka kompetentingos institucijos.

3. Specialiąją sąsają įdiegę sąskaitas tvarkantys mokėjimo paslaugų teikėjai turi užtikrinti, kad ši sąsaja nedarytų kliūčių mokėjimo inicijavimo paslaugų ir informavimo apie sąskaitas paslaugų teikimui. Tokios kliūtys, be kita ko, gali būti kliudymas 30 straipsnio 1 dalyje nurodytiems mokėjimo paslaugų teikėjams naudoti požymius, kuriuos sąskaitas tvarkantys mokėjimo paslaugų teikėjai pateikė savo klientams; sąskaitą tvarkančio mokėjimo paslaugų teikėjo vykdomo autentiškumo patvirtinimo ar kitų funkcijų peradresavimas; papildomų leidimų ir registracijų, be numatytųjų Direktyvos (ES) 2015/2366 11, 14 ir 15 straipsniuose, reikalavimas arba reikalavimas papildomai patikrinti sutikimą, kurį mokėjimo paslaugų vartotojai suteikė mokėjimo inicijavimo paslaugų teikėjams ir informavimo apie sąskaitas paslaugų teikėjams.

4. Taikydami 1 ir 2 dalis, sąskaitas tvarkantys mokėjimo paslaugų teikėjai atlieka specialiosios sąsajos prieinamumo ir veiksmingumo stebėjimą. Savo interneto svetainėje sąskaitas tvarkantys mokėjimo paslaugų teikėjai skelbia specialiosios sąsajos ir mokėjimo paslaugų vartotojų naudojamos sąsajos prieinamumo ir veiksmingumo ketvirčio ataskaitas.

33 straipsnis

Specialiajai sąsajai skirtos nenumatytų atvejų priemonės

1. Sąskaitas tvarkantys mokėjimo paslaugų teikėjai į specialiosios sąsajos projektą įtraukia nenumatytų atvejų priemonių strategijas ir planus, skirtus atvejams, kai sąsajos veiksmingumas neatitinka 32 straipsnio, kai sąsaja neplanuotai tampa neprieinama ir kai sistemos sugenda. Laikoma, kad sąsaja tapo neplanuotai neprieinama arba kad sistemos sugedo, kai per 30 sekundžių neatsakoma į iš eilės pateiktus penkis prašymus gauti informacijos, reikalingos mokėjimo inicijavimo paslaugai arba informavimo apie sąskaitas paslaugai suteikti.

2. Nenumatytų atvejų priemonės apima ryšių planus informuoti mokėjimo paslaugų teikėjus, kurie naudojasi specialiąja sąsaja, apie sistemos atkūrimo priemones ir nedelsiant prieinamų alternatyvų, kuriomis mokėjimo paslaugų teikėjai tuo metu gali naudotis, aprašymą.

3. Tiek sąskaitą tvarkantis mokėjimo paslaugų teikėjas, tiek 30 straipsnio 1 dalyje nurodyti mokėjimo paslaugų teikėjai nedelsdami praneša apie specialiųjų sąsajų problemas, nurodytas 1 dalyje, savo atitinkamoms kompetentingoms nacionalinėms institucijoms.

4. Taikant nenumatytų atvejų mechanizmą, 30 straipsnio 1 dalyje nurodytiems mokėjimo paslaugų teikėjams leidžiama naudotis sąsajomis, suteiktomis mokėjimo paslaugų vartotojams autentiškumo patvirtinimui ir ryšiams su jų sąskaitą tvarkančiu mokėjimo paslaugų teikėju, kol specialioji sąsaja atkuriama taip, kad jos prieinamumo ir veiksmingumo lygis atitiktų nurodytąjį 32 straipsnyje.

5. Tuo tikslu sąskaitas tvarkantys mokėjimo paslaugų teikėjai užtikrina, kad 30 straipsnio 1 dalyje nurodyti mokėjimo paslaugų teikėjai galėtų būti identifikuojami ir galėtų pasikliauti autentiškumo patvirtinimo procedūromis, kurias sąskaitą tvarkantis mokėjimo paslaugų teikėjas teikia mokėjimo paslaugų vartotojui. Naudodamiesi 4 dalyje nurodyta sąsaja, 30 straipsnio 1 dalyje nurodyti mokėjimo paslaugų teikėjai:

a) imasi visų priemonių, kurių reikia siekiant užtikrinti, kad jie neprieitų prie duomenų, jų nesaugotų ar netvarkytų kitais tikslais nei teikdami paslaugą, kurios prašo mokėjimo paslaugų vartotojas;

b) toliau laikosi atitinkamų Direktyvos (ES) 2015/2366 66 straipsnio 3 dalyje ir 67 straipsnio 2 dalyje nurodytų pareigų;

c) įrašo duomenis, prie kurių prieinama naudojantis sąsaja, kurią sąskaitą tvarkantis mokėjimo paslaugų teikėjas teikia savo mokėjimo paslaugų vartotojams, ir paprašius be reikalo nedelsdami pateikia įrašų žurnalo rinkmenas savo nacionalinėms kompetentingoms institucijoms;

d) paprašius be reikalo nedelsdami savo nacionalinėms kompetentingoms institucijoms deramai pagrindžia sąsajos, pateiktos mokėjimo paslaugų vartotojams, kad galėtų tiesiogiai internetu jungtis prie savo mokėjimo sąskaitos, naudojimą;

e) atitinkamai informuoja sąskaitą tvarkantį mokėjimo paslaugų teikėją.

6. Pasikonsultavusios su EBI ir siekdamos užtikrinti, kad toliau nurodytos sąlygos būtų nuosekliai taikomos, kompetentingos institucijos atleidžia specialiąją sąsają pasirinkusius sąskaitas tvarkančius mokėjimo paslaugų teikėjus nuo pareigos nustatyti 4 dalyje nurodytą nenumatytų atvejų mechanizmą, kai specialioji sąsaja atitinka visas šias sąlygas:

a) atitinka visus specialiosioms sąsajoms taikomus reikalavimus pagal 32 straipsnį;

b) yra sukurta ir testuota pagal 30 straipsnio 5 dalį, o testavimo rezultatai tenkino čia minėtų mokėjimo paslaugų teikėjų reikalavimus;

c) buvo mokėjimo paslaugų teikėjų plačiai naudojama bent tris mėnesius teikiant informavimo apie sąskaitas paslaugas, mokėjimo inicijavimo paslaugas ir disponavimo lėšomis patvirtinimo kortele grindžiamiems mokėjimams paslaugas;

d) visos su specialiąja sąsaja susijusios problemos buvo išspręstos be reikalo nedelsiant.

7. Kompetentingos institucijos atšaukia 6 dalyje nurodytą išimtį, jeigu sąskaitas tvarkantys mokėjimo paslaugų teikėjai nevykdo a ir d punktų sąlygų daugiau nei dvi iš eilės einančias kalendorines savaites. Kompetentingos institucijos apie šį išimties atšaukimą informuoja EBI ir užtikrina, kad sąskaitą tvarkantis mokėjimo paslaugų teikėjas kuo skubiau, bet ne vėliau kaip per du mėnesius, nustatytų 4 dalyje nurodytą nenumatytų atvejų mechanizmą.

34 straipsnis

Sertifikatai

1. Tam, kad identifikuotųsi, kaip nurodyta 30 straipsnio 1 dalies a punkte, mokėjimo paslaugų teikėjai naudoja kvalifikuotus elektroninio spaudo sertifikatus, kaip nurodyta Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 3 straipsnio 30 dalyje, arba interneto svetainių tapatumo nustatymo sertifikatus, kaip nurodyta to reglamento 3 straipsnio 39 dalyje.

2. Taikant šį reglamentą, registracijos numeris, nurodomas oficialiuose įrašuose pagal Reglamento (ES) Nr. 910/2014 III priedo c punktą arba IV priedo c punktą, yra mokėjimo paslaugų teikėjų, išleidžiančių kortele grindžiamas mokėjimo priemones, informavimo apie sąskaitas paslaugų teikėjų ir mokėjimo inicijavimo paslaugų teikėjų, įskaitant tokias paslaugas teikiančius sąskaitas tvarkančius mokėjimo paslaugų teikėjus, leidimo numeris, įtrauktas į buveinės valstybės narės viešąjį registrą pagal Direktyvos (ES) 2015/2366 14 straipsnį arba paimtas iš pranešimų apie kiekvieną leidimą, suteiktą pagal Europos Parlamento ir Tarybos direktyvos 2013/36/ES ([1]) 8 straipsnį laikantis tos direktyvos 20 straipsnio.

3. Taikant šį reglamentą, 1 dalyje nurodyti kvalifikuoti elektroninio spaudo sertifikatai arba interneto svetainių tapatumo nustatymo sertifikatai tarptautinių finansų sričiai įprasta kalba turi papildomus specifinius požymius, susijusius su:

a) mokėjimo paslaugų teikėjo funkcija, kurią gali sudaryti viena ar kelios iš šių:

   i) sąskaitos tvarkymas;

   ii) mokėjimo inicijavimas;

   iii) sąskaitos informacija;

   iv) kortele grindžiamų mokėjimo priemonių išdavimas;

b) kompetentingų institucijų, kuriose registruotas mokėjimo paslaugų teikėjas, pavadinimu.

4. 3 dalyje nurodyti požymiai nedaro poveikio kvalifikuotų elektroninio spaudo sertifikatų arba interneto svetainių tapatumo nustatymo sertifikatų sąveikumui ir pripažinimui.

([1]) 2013 m. birželio 26 d. Europos Parlamento ir Tarybos direktyva 2013/36/ES dėl galimybės verstis kredito įstaigų veikla ir dėl riziką ribojančios kredito įstaigų ir investicinių įmonių priežiūros, kuria iš dalies keičiama Direktyva 2002/87/EB ir panaikinamos direktyvos 2006/48/EB bei 2006/49/EB (OL L 176, 2013 6 27, p. 338).

35 straipsnis

Ryšių seanso saugumas

1. Siekiant apsaugoti duomenų konfidencialumą ir vientisumą, sąskaitas tvarkantys mokėjimo paslaugų teikėjai, mokėjimo paslaugų teikėjai, išleidžiantys kortele grindžiamas mokėjimo priemones, informavimo apie sąskaitas paslaugų teikėjai ir mokėjimo inicijavimo paslaugų teikėjai užtikrina, kad keičiantis duomenimis internetu visą atitinkamą ryšių seansą šalių ryšiams būtų taikomas saugus šifravimas naudojant patikimas ir visuotinai pripažintas šifravimo technologijas.

2. Mokėjimo paslaugų teikėjai, išleidžiantys kortele grindžiamas mokėjimo priemones, informavimo apie sąskaitas paslaugų teikėjai ir mokėjimo inicijavimo paslaugų teikėjai stengiasi, kad sąskaitas tvarkančių mokėjimo paslaugų teikėjų teikiami prieigos seansai būtų kuo trumpesni, ir aktyviai tokius seansus nutraukia, kai tik prašomas veiksmas atliekamas.

3. Vienu metu palaikydami kelis tinklo seansus su sąskaitą tvarkančiu mokėjimo paslaugų teikėju, informavimo apie sąskaitas paslaugų teikėjai ir mokėjimo inicijavimo paslaugų teikėjai užtikrina, kad šie seansai būtų saugiai susieti su atitinkamais seansais, pradėtais su mokėjimo paslaugų vartotoju (-ais), siekiant užkirsti kelią klaidingam bet kurio pranešimo ar informacijos, kuriais keičiamasi, nukreipimui.

4. Informavimo apie sąskaitas paslaugų teikėjai, mokėjimo inicijavimo paslaugų teikėjai ir mokėjimo paslaugų teikėjai, išleidžiantys kortele grindžiamas mokėjimo priemones, palaikydami ryšius su sąskaitą tvarkančiu mokėjimo paslaugų teikėju, naudoja vienareikšmes nuorodas, žyminčias:

a) mokėjimo paslaugų vartotoją (-us) ir atitinkamą ryšių seansą siekiant atskirti kelis to paties mokėjimo paslaugų vartotojo (-ų) prašymus;

b) mokėjimo inicijavimo paslaugų atveju – inicijuotą mokėjimo operaciją, kuriai suteiktas unikalus identifikatorius;

c) disponavimo lėšomis patvirtinimo atveju – prašymą, susijusį su suma, reikalinga kortele grindžiamai mokėjimo operacijai įvykdyti, kuriam suteiktas unikalus identifikatorius.

5. Sąskaitas tvarkantys mokėjimo paslaugų teikėjai, informavimo apie sąskaitas paslaugų teikėjai, mokėjimo inicijavimo paslaugų teikėjai ir mokėjimo paslaugų teikėjai, išleidžiantys kortele grindžiamas mokėjimo priemones, užtikrina, kad jokie jų darbuotojai niekada neturėtų galimybės tiesiogiai ar netiesiogiai perskaityti perduodamų personalizuotų saugumo požymių ir atpažinties kodų.

Jeigu jų kompetencijai priklausančių personalizuotų saugumo požymių konfidencialumas pažeidžiamas, atitinkami teikėjai nedelsdami informuoja su tais požymiais susijusį mokėjimo paslaugų vartotoją ir personalizuotų saugumo požymių išdavėją.

36 straipsnis

Keitimasis duomenimis

1. Sąskaitas tvarkantys mokėjimo paslaugų teikėjai laikosi visų šių reikalavimų:

a) jie pateikia informavimo apie sąskaitas paslaugų teikėjams tą pačią informaciją apie nurodytas mokėjimo sąskaitas ir susijusias mokėjimo operacijas, kuri yra pateikiama mokėjimo paslaugų vartotojui, kai jis tiesiogiai prašo prieigos prie sąskaitos informacijos, jeigu ši informacija neapima neskelbtinų mokėjimo duomenų;

b) iš karto po to, kai gavo mokėjimo nurodymą, jie pateikia mokėjimo inicijavimo paslaugų teikėjams tą pačią informaciją apie mokėjimo operacijos inicijavimą ir įvykdymą, kurią pateikia arba parodo mokėjimo paslaugų vartotojui, kai šis operaciją inicijuoja tiesiogiai;

c) gavę prašymą jie iš karto pateikia mokėjimo paslaugų teikėjams patvirtinimą paprastu „taip“ arba „ne“ atsakymu, nurodydami, ar suma, reikalinga mokėjimo operacijai įvykdyti, yra mokėtojo mokėjimo sąskaitoje.

2. Identifikavimo, autentiškumo patvirtinimo arba keitimosi duomenų elementais metu įvykus nenumatytam įvykiui ar klaidai, sąskaitą tvarkantis mokėjimo paslaugų teikėjas nusiunčia mokėjimo inicijavimo paslaugų teikėjui arba informavimo apie sąskaitas paslaugų teikėjui ir mokėjimo paslaugų teikėjui, išleidžiančiam kortele grindžiamas mokėjimo priemones, pranešimą, kuriame paaiškina nenumatyto įvykio ar klaidos priežastis.

Kai pagal 32 straipsnį sąskaitą tvarkantis mokėjimo paslaugų teikėjas teikia specialiąją sąsają, toje sąsajoje yra numatyti pranešimai apie nenumatytus įvykius ar klaidas, kuriuos bet kuris mokėjimo paslaugų teikėjas, aptikęs įvykį ar klaidą, siunčia kitiems mokėjimo paslaugų teikėjams, dalyvaujantiems ryšių seanse.

3. Informavimo apie sąskaitas paslaugų teikėjai įdiegia tinkamus ir veiksmingus mechanizmus, kuriais užkertamas kelias prieigai prie informacijos, išskyrus prieigą iš nurodytų mokėjimo sąskaitų ir susijusių mokėjimo operacijų, kai yra gautas aiškus vartotojo sutikimas.

4. Mokėjimo inicijavimo paslaugų teikėjas suteikia sąskaitas tvarkantiems mokėjimo paslaugų teikėjams tą pačią informaciją, kurios prašoma iš mokėjimo paslaugų vartotojo, kai šis tiesiogiai inicijuoja mokėjimo operaciją.

5. Informavimo apie sąskaitas paslaugų teikėjai turi prieigą prie informacijos iš nurodytų mokėjimo sąskaitų ir susijusių mokėjimo operacijų, kurią saugo sąskaitas tvarkantys mokėjimo paslaugų teikėjai siekdami teikti informavimo apie sąskaitas paslaugą bet kuriuo iš šių atvejų:

a) kai mokėjimo paslaugų vartotojas aktyviai tokios informacijos prašo;

b) kai mokėjimo paslaugų vartotojas aktyviai tokios informacijos neprašo, ne dažniau kaip keturis kartus per 24 valandų laikotarpį, išskyrus atvejus, kai informavimo apie sąskaitas paslaugų teikėjas ir sąskaitą tvarkantis mokėjimo paslaugų teikėjas susitaria dėl kitokio periodiškumo ir gauna tam mokėjimo paslaugų vartotojo sutikimą.

VI SKYRIUS

BAIGIAMOSIOS NUOSTATOS

37 straipsnis

Peržiūra

Nedarant poveikio Direktyvos (ES) 2015/2366 98 straipsnio 5 dalies taikymui, EBI peržiūri 2021 m. kovo 14 d. šio reglamento priede nurodytus sukčiavimo rodiklius ir pagal 33 straipsnio 6 dalį suteiktas išimtis, susijusias su specialiosiomis sąsajomis, ir prireikus atnaujintus jų projektus pagal Reglamento (ES) Nr. 1093/2010 10 straipsnį pateikia Komisijai.

38 straipsnis

Įsigaliojimas

1. Šis reglamentas įsigalioja kitą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

2. Šis reglamentas taikomas nuo 2019 m. rugsėjo 14 d.

3. Tačiau 30 straipsnio 3 ir 5 dalys taikomos nuo 2019 m. kovo 14 d.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje 2017 m. lapkričio 27 d.

Komisijos vardu

Pirmininkas

Jean-Claude JUNCKER

PRIEDAS

	Orientacinis sukčiavimo rodiklis (%)	
Išimties ribinė vertė	Nuotoliniai elektroniniai kortele grindžiami mokėjimai	Nuotoliniai elektroniniai kredito pervedimai
500 EUR	0,01	0,005
250 EUR	0,06	0,01
100 EUR	0,13	0,015