EBA/GL/2014/12_Rev1

2014 m. gruodžio 19 d.

Galutinės gairės

dėl mokėjimų internetu saugumo

Turinys

Gairės dėl mokėjimų internetu saugumo

Gairių statusas

Šiame dokumente pateikiamos gairės, parengtos pagal 2010 m. lapkričio 24 d. Europos Parlamento ir Tarybos reglamento (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 (*EBI reglamentas*), 16 straipsnį. Pagal EBI reglamento 16 straipsnio 3 dalį kompetentingos institucijos ir finansų įstaigos privalo dėti visas pastangas laikytis šių gairių.

Gairėse išdėstoma EBI nuomonė apie tai, kokios priežiūros praktikos turėtų būti laikomasi Europos finansų priežiūros sistemoje arba kaip konkrečioje srityje reikėtų taikyti Sąjungos teisę. Todėl EBI tikisi, kad visos kompetentingos institucijos ir finansų įstaigos laikysis joms skirtų gairių. Kompetentingos institucijos, kurioms taikomos šios gairės turėtų jų laikytis atitinkamai jas įtraukdamos į savo priežiūros praktiką (pvz., pakeisti savo teisinę sistemą arba priežiūros procesus), įskaitant ir tuos atvejus, kai gairės visų pirma skirtos įstaigoms.

Pranešimo teikimo reikalavimai

Pagal EBI reglamento 16 straipsnio 3 dalį kompetentingos institucijos iki 2015 m. gegužės 5 d. privalo EBI pranešti, ar jos laikosi arba ketina laikytis šių gairių, arba nurodyti nesilaikymo priežastis. Negavusi pranešimo iki šio termino pabaigos, EBI laikys, kad kompetentinga institucija šių gairių nesilaiko. Pranešimai turėtų būti teikiami nusiunčiant 5 skyriuje nustatytą formą adresu compliance@eba.europa.eu ir pateikiant nuorodą „EBA/GL/2014/12“. Pranešimus turėtų teikti asmenys, turintys atitinkamos institucijos įgaliojimus pranešti apie gairių laikymąsi savo kompetentingos institucijos vardu.

Pranešimai pagal EBI reglamento 16 straipsnio 3 dalį bus skelbiami EBI interneto svetainėje.

I dalis. Taikymo sritis ir apibrėžtys

Taikymo sritis

1. Šiose gairėse nustatyti būtiniausi internetu atliekamų mokėjimų saugumo reikalavimai. Gairės parengtos remiantis Direktyvos 2007/64/EB[1] (toliau – Mokėjimo paslaugų direktyva, MPD) taisyklėmis dėl informavimo reikalavimų, taikomų mokėjimo paslaugoms ir mokėjimo paslaugų teikėjų (toliau – MPT) pareigoms, susijusioms su mokėjimo paslaugų teikimu. Be to, Direktyvos 10 straipsnio 4 dalyje reikalaujama, kad mokėjimo įstaigos turėtų tvirtą mokėjimo paslaugų veiklos valdymo tvarką ir atitinkamus vidaus kontrolės mechanizmus.

2. Gairės taikomos mokėjimo paslaugų teikimui, kai Direktyvos 1 straipsnyje nurodyti MPT siūlo šias paslaugas internetu.

3. Gairės skirtos finansų įstaigoms, apibrėžtoms Reglamento (ES) Nr. 1093/2010 4 straipsnio 1 dalyje, ir kompetentingoms institucijoms, apibrėžtoms Reglamento (ES) Nr. 1093/2010 4 straipsnio 2 dalyje. 28 Europos Sąjungos valstybių narių kompetentingos institucijos turėtų užtikrinti, kad MPD apibrėžti ir jų prižiūrimi MPT taikytų šias gaires.

4. Be to, kompetentingos institucijos gali nuspręsti reikalauti, kad MPT kompetentingai institucijai praneštų, jog laikosi šių gairių.

5. Šiomis gairėmis nekeičiamas Europos Centrinio Banko internetu atliekamų mokėjimų saugumo rekomendacijų[2] (toliau – pranešimas) galiojimas. Pranešimas ir toliau yra dokumentas, kuriuo vadovaudamiesi centriniai bankai, vykdydami mokėjimo sistemų ir priemonių priežiūrą, turėtų vertinti atitiktį mokėjimų internetu saugumo reikalavimams.

6. Gairėse išdėstyti būtiniausi lūkesčiai. Gairėmis nekeičiama MPT pareiga stebėti ir vertinti su savo atliekamomis mokėjimo operacijomis susijusią riziką, parengti išsamią savo saugumo politiką ir įgyvendinti pakankamas saugumo, specialiąsias, incidentų valdymo ir veiklos tęstinumo priemones, kurios atitiktų teikiamoms mokėjimų paslaugoms būdingą riziką.

7. Šių gairių tikslas – nustatyti bendrus būtiniausius reikalavimus, taikytinus toliau išvardytoms mokėjimų internetu paslaugoms, nepaisant to, koks prieigos įrenginys naudojamas:

    - [kortelės] mokėjimų internetu kortele, įskaitant mokėjimus virtualiąja kortele, ir mokėjimų kortele duomenų registravimo, kad šiuos duomenis būtų galima naudoti skaitmeninės piniginės sprendimams, paslaugoms;

[1] 2007 m. lapkričio 13 d. Europos Parlamento ir Tarybos direktyva 2007/64/ES dėl mokėjimo paslaugų vidaus rinkoje, iš dalies keičianti direktyvas 97/7/EB, 2002/65/EB, 2005/60/EB ir 2006/48/EB ir panaikinanti Direktyvą 97/5/EB (OL L 319, 2007 12 5).

[2] http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html.

- [kredito pervedimai] kredito pervedimų (angl. *credit transfer*, CT) internetu paslaugoms;

- [e. įgaliojimas] elektroninių tiesioginio debeto įgaliojimų suteikimo ir keitimo paslaugoms;

- [e. pinigai] elektroninių pinigų pervedimo tarp dviejų e. pinigų sąskaitų internetu paslaugoms.

8. Kiekvieną gairėse nurodytą rezultatą galima pasiekti įvairiomis priemonėmis. Šiose gairėse pateikiami ne tik toliau išdėstyti reikalavimai, bet ir geriausios patirties pavyzdžiai (1 priedas), kuriais vadovautis MPT siūloma, bet neprivaloma.

9. Jeigu mokėjimo paslaugas ir priemones siūloma teikti per mokėjimų schemą (pavyzdžiui, mokėjimų kortele schema, kredito pervedimo schema, tiesioginio debeto schema ir pan.), kompetentingos institucijos ir atitinkamas centrinis bankas, kuris vykdo mokėjimo priemonių priežiūros funkciją, turėtų palaikyti ryšius ir užtikrinti, kad už šios schemos veikimą atsakingi rinkos dalyviai nuosekliai taikytų šias gaires.

10. Mokėjimų integruotojai[3], siūlantys mokėjimo inicijavimo paslaugas, yra laikomi mokėjimo internetu paslaugų priemonių priėmėjais (taigi – MPT) arba atitinkamų schemų ar MPT išorės techninių paslaugų teikėjais. Antruoju atveju iš mokėjimų integruotojų pagal sutartį turėtų būti reikalaujama laikytis šių gairių.

11. Šios gairės netaikomos:

- kitoms MPT per savo mokėjimų interneto svetainę internetu teikiamoms paslaugoms (pavyzdžiui, e. maklerio, internetinių sutarčių);

- mokėjimams, kurių nurodymai pateikiami paštu, telefonu, balso paštu arba naudojant SMS žinutėmis pagrįstas technologines priemones;

- mokėjimams mobiliaisiais telefonais, išskyrus per interneto naršyklę inicijuojamus mokėjimus;

- kredito pervedimams, kai trečioji šalis prisijungia prie vartotojo mokėjimo sąskaitos;

- mokėjimo operacijoms, kurias įmonė vykdo per specializuotus tinklus;

[3] Mokėjimų integruotojai mokėjimo gavėjui (t. y. elektroninės prekybos vykdytojui) suteikia standartizuotą sąsają su MPT teikiamomis mokėjimų inicijavimo paslaugomis.

- mokėjimams kortele, kai naudojamos anonimiškos, nepapildomosios fizinės arba virtualiosios išankstinio mokėjimo kortelės, o kortelę išdavusio MPT ir kortelės turėtojo santykiai nėra nuolatiniai;

- mokėjimų operacijoms tarpuskaitos ir atsiskaitymų schemose.

Apibrėžtys

12. Šiose gairėse greta MPD apibrėžtų sąvokų vartojamos šios sąvokos:

- *Autentiškumo patvirtinimas* – procedūra, per kurią MPT patikrina vartotojo tapatybę.

- *Griežtas vartotojo autentiškumo patvirtinimas* – šiose gairėse tai procedūra, per kurią naudojami du arba daugiau iš toliau išvardytų elementų, suskirstytų į žinojimo, turėjimo ir būdingumo kategorijas: i) elementas, kurį žino tik vartotojas, pavyzdžiui, pastovus slaptažodis, kodas, asmens identifikavimo numeris; ii) elementas, kurį turi tik vartotojas, pavyzdžiui, prieigos raktas, lustinė kortelė, mobilusis telefonas; iii) tik vartotojui būdingas elementas, pavyzdžiui, biometriniai ypatumai – pirštų atspaudas ar pan. Be to, pasirinkti elementai turi būti vienas nuo kito nepriklausomi, tai yra pažeidus vieną neturėtų būti pažeistas kitas (-i). Bent vieno iš elementų neturėtų būti galima panaudoti pakartotinai ir atkurti (išskyrus būdingumo elementą), ir jo neturėtų būti galima slapta pavogti internetu. Griežto autentiškumo patvirtinimo procedūra turėtų būti suplanuota taip, kad būtų apsaugotas autentiškumui patvirtinti naudojamų duomenų konfidencialumas.

- *Autorizavimas* – procedūra, per kurią tikrinama, ar vartotojas arba MPT turi teisę atlikti tam tikrą veiksmą, pavyzdžiui, pervesti lėšas arba prieiti prie neskelbtinų duomenų.

- *Asmens duomenys* – informacija (dažniausiai konfidenciali), kurią vartotojas arba MPT pateikia autentiškumui patvirtinti. Prie asmens duomenų taip pat galima priskirti fizinę priemonę su informacija (pavyzdžiui, vienkartinio slaptažodžio generatorius, lustinė kortelė) arba dalyką, kurį vartotojas įsimena arba kuris jam yra būdingas (pavyzdžiui, biometrinės savybės).

- *Didelis mokėjimų saugumo incidentas* – incidentas, dėl kurio padaromas arba gali būti padarytas reikšmingas poveikis su mokėjimais susijusių MPT sistemų saugumui, vientisumui arba tęstinumui ir (arba) neskelbtinų mokėjimo duomenų arba lėšų saugumui. Vertinant reikšmingumą reikėtų atsižvelgti į galimai nukentėjusių vartotojų skaičių, sumą, kuriai kilo rizika, ir poveikį kitiems MPT arba kitai mokėjimo infrastruktūrai.

- *Operacijos rizikos analizė* – su konkrečia operacija susijusios rizikos vertinimas, atsižvelgiant į tokius kriterijus kaip, pavyzdžiui, vartotojo mokėjimų modeliai (elgsena), atitinkamos operacijos suma, produkto rūšis ir mokėjimo gavėjo pobūdis.

- *Virtualiosios kortelės* – kortelės principu grindžiamas mokėjimo sprendimas, pagal kurį suteikiamas alternatyvios, laikinos, trumpesnio galiojimo, riboto naudojimo kortelės su iš anksto nustatyta išlaidų riba numeris, kurį galima naudoti perkant internetu.

- *Skaitmeninės piniginės sprendimai* – sprendimai, kuriais vartotojui suteikiama galimybė užregistruoti vienos arba kelių mokėjimo priemonių duomenis, kad galėtų atlikti mokėjimus keletui elektroninės prekybos vykdytojų.

II dalis. Gairės dėl mokėjimų internetu saugumo

Bendroji kontrolės ir saugumo aplinka

Valdymas

1. MPT turėtų laikytis oficialios mokėjimų internetu paslaugų saugumo politikos ir šią politiką reguliariai peržiūrėti.

   1.1 Saugumo politika turėtų būti tinkamai dokumentuota, reguliariai peržiūrima (pagal 2.4 gairę) ir patvirtinta vyresniosios vadovybės. Joje turėtų būti nustatyti saugumo tikslai ir toleruotinas rizikos lygis.

   1.2 Saugumo politikos nuostatomis turėtų būti apibrėžtos funkcijos ir atsakomybė, tarp jų – rizikos valdymo funkcija su tiesiogine atskaitomybe valdybos lygmens organui, atskaitomybė už suteiktas mokėjimų internetu paslaugas, įskaitant neskelbtinų mokėjimų duomenų valdymą rizikos vertinimo, kontrolės ir mažinimo atžvilgiu.

Rizikos vertinimas

2. Prieš pradėdami teikti paslaugą (-as) MPT turėtų įvertinti internetu atliekamų mokėjimų ir susijusių paslaugų saugumo riziką ir šį vertinimą kruopščiai dokumentuoti, o vėliau tai daryti reguliariai.

   2.1 MPT, atlikdami rizikos valdymo funkciją, turėtų išsamiai vertinti mokėjimų internetu ir susijusių paslaugų riziką ir šį vertinimą dokumentuoti. MPT turėtų nagrinėti nuolat vykdomos grėsmių šių MPT teikiamų arba planuojamų teikti mokėjimų internetu paslaugų saugumui stebėsenos rezultatus, atsižvelgdami į: i) tai, kokius technologinius sprendimus naudoja; ii) paslaugas, kurios perduodamos teikti išorės teikėjams; iii) vartotojų techninę aplinką. MPT turėtų nagrinėti ir su savo pačių[4], ir su vartotojų[5] pasirinktomis technologinėmis platformomis, taikomųjų programų architektūra, programavimo metodais ir tvarka susijusią riziką, taip pat saugumo incidentų stebėsenos proceso rezultatus (žr. 3 gairę).

   2.2 Tuo remdamiesi MPT turėtų nustatyti, ar gali prireikti ir kokia apimtimi gali prireikti keisti esamas saugumo priemones, naudojamas technologijas ir procedūras arba siūlomas paslaugas. MPT turėtų atsižvelgti į tai, kiek laiko reikės pakeitimams įgyvendinti (įskaitant tai, kiek vartotojams reikės laiko jiems įdiegti), ir imtis reikiamų

[4] Pavyzdžiui, pažeidžiamas sistemos vietas, dėl kurių gali būti perimtas seansas (angl. *session hijacking*), pasinaudota SQL intarpais (angl. *SQL injection*), į vartotojo peržiūrimą puslapį įterptas programinis kodas (angl. *cross-site scripting*), perpildyta atmintis (angl. *buffer overflow*) ir pan.

[5] Pavyzdžiui, riziką, susijusią su daugialypės terpės taikomųjų programų, naršyklės papildinių, kadrų, išorės sąsajų naudojimu ir pan.

tarpinių priemonių, kad kiek galėdami sumažintų saugumo incidentų ir sukčiavimo atvejų skaičių, taip pat galimus žalingus padarinius.

2.3 Vertinant riziką reikėtų atsižvelgti į poreikį neatskleisti neskelbtinų mokėjimų duomenų ir juos saugoti.

2.4 MPT turėtų įsipareigoti peržiūrėti rizikos scenarijus ir esamas saugumo priemones po didelių incidentų, per kuriuos paveikiamos jų paslaugos, prieš didelius infrastruktūros arba procedūrų pakeitimus ir tada, kai vykdant rizikos stebėseną nustatoma naujų grėsmių. Be to, bent kartą per metus turėtų būti atliekama bendroji rizikos vertinimo peržiūra. Rizikos vertinimų ir peržiūrų rezultatai turėtų būti teikiami vyresniajai vadovybei tvirtinti.

Incidentų stebėsena ir pranešimas apie juos

3. MPT turėtų užtikrinti, kad būtų vykdoma nuosekli kompleksinė stebėsena, sprendžiami saugumo incidentų klausimai ir imamasi paskesnių priemonių, įskaitant vartotojų skundų dėl saugumo nagrinėjimą. MPT turėtų nustatyti pranešimo apie šiuos incidentus vadovybei, o kilus dideliems mokėjimų saugumo incidentams – kompetentingoms institucijoms tvarką.

3.1 MPT turėtų būti įdiegę tvarką, pagal kurią vykdytų saugumo incidentų stebėseną, spręstų saugumo incidentų klausimus, imtųsi paskesnių priemonių dėl saugumo incidentų, nagrinėtų vartotojų skundus dėl saugumo ir praneštų apie tokius incidentus vadovybei.

3.2 MPT turėtų būti parengę tvarką, pagal kurią nedelsdami kompetentingoms institucijoms (t. y. priežiūros ir duomenų apsaugos institucijoms), jeigu tokios institucijos yra įsteigtos, praneštų apie didelius mokėjimų saugumo incidentus, susijusius su teikiamomis mokėjimų paslaugomis.

3.3 MPT turėtų būti parengę tvarką, pagal kurią bendradarbiautų su atitinkamomis teisėsaugos įstaigomis didelių mokėjimų saugumo incidentų, įskaitant duomenų saugumo pažeidimus, klausimais.

3.4 Mokėjimo priemones priimantys MPT turėtų sutartyje iš elektroninės prekybos vykdytojų, kurie laiko, tvarko arba perduoda neskelbtinus mokėjimų duomenis, reikalauti bendradarbiauti kilus dideliems mokėjimų saugumo incidentams, įskaitant duomenų saugumo pažeidimus, ir su MPT, ir su atitinkamomis teisėsaugos įstaigomis. Jeigu MPT sužino, kad elektroninės prekybos vykdytojas nebendradarbiauja taip, kaip reikalaujama pagal sutartį, jis turėtų imtis priemonių ir priversti laikytis šios sutartyje nustatytos pareigos arba nutraukti sutartį.

Rizikos kontrolė ir mažinimas

4. MPT, vadovaudamiesi atitinkama savo saugumo politika, turėtų įgyvendinti saugumo priemones ir mažinti nustatytą riziką. Šias priemones turėtų sudaryti kelių pakopų apsaugos priemonės, kad pažeidus vieną apsaugos pakopą apsauga būtų užtikrinta paskesne apsaugos pakopa (kelių pakopų apsauga).

4.1 Projektuodami, kurdami ir palaikydami mokėjimų internetu paslaugas MPT turėtų ypač atkreipti dėmesį į tai, kad pareigos, susijusios su informacinių technologijų (IT) aplinka (pavyzdžiui, projektavimo, testavimo ir darbine) ir tinkamu „mažiausios privilegijos“ principo, kuriuo grindžiamas geras tapatybės ir prieigos valdymas, įgyvendinimu būtų pakankamai atskirtos[6].

4.2 MPT turėtų būti įdiegę reikiamus saugumo sprendimus, kad apsaugotų tinklus, interneto svetaines, serverius ir ryšio linijas nuo piktnaudžiavimo arba atakų. MPT turėtų panaikinti visas perteklines serverių funkcijas, kad šiuos serverius apsaugotų (sutvirtintų), ir ištaisyti arba sumažinti pažeidžiamas taikomųjų programų vietas, dėl kurių kyla rizika. Prieiga prie duomenų ir išteklių per įvairias taikomąsias programas turėtų būti minimali, laikantis „mažiausios privilegijos“ principo. Siekiant apriboti suklastotų interneto svetainių (kuriomis imituojamos teisėtos MPT svetainės) naudojimą, interneto sandorių svetainių, kuriose siūlomos mokėjimų internetu paslaugos, tapatumas turėtų būti nustatomas pagal MPT vardu išduotus išplėstinio patvirtinimo sertifikatus (angl. *extended validation certificates*) arba kitais panašiais autentiškumo patvirtinimo metodais.

4.3 MPT turėtų būti nustatę reikiamą tvarką, pagal kurią stebėtų, sektų ir ribotų prieigą prie: i) neskelbtinų mokėjimų duomenų ir ii) loginių ir fizinių ypatingos svarbos išteklių, pavyzdžiui, tinklų, sistemų, duomenų bazių, saugumo modulių ir pan. MPT turėtų sukurti, saugoti ir analizuoti atitinkamus prisijungimo ir veiksmų įrašus.

4.4 Projektuodami[7], kurdami ir palaikydami mokėjimų internetu paslaugas, MPT turėtų užtikrinti, kad svarbiausias pagrindinių funkcijų principas būtų duomenų minimizavimas[8]: reikėtų rinkti, reikiamais kanalais teikti, tvarkyti, laikyti ir (arba) archyvuoti ir vaizdinėmis priemonėmis išreikšti tik minimalų neskelbtinų duomenų kiekį.

4.5 Mokėjimų internetu paslaugų saugumo priemonės turėtų būti testuojamos prižiūrint rizikos valdymo funkcijas vykdantiems asmenims, siekiant užtikrinti, kad šios

[6] „Kiekvienoje programoje reikėtų naudotis ir kiekvienas privilegijuotasis sistemos naudotojas turėtų naudotis mažiausiu skaičiumi privilegijų, reikalingų darbui užbaigti“. Žr. Saltzer, J. H. (1974), „Protection and the Control of Information Sharing in Multics“, leidinio „Communications of the ACM“ 17 tomas, Nr. 7, p. 388.

[7] Privatumo užtikrinimas projektuojant.

[8] Duomenų minimizavimas – politika, kurios laikantis renkamas mažiausias tam tikrai funkcijai atlikti reikalingas asmeninės informacijos kiekis.

priemonės būtų patikimos ir veiksmingos. Visi pakeitimai turėtų būti atliekami laikantis oficialios pakeitimų valdymo tvarkos, siekiant užtikrinti, kad jie būtų tinkamai suplanuoti, ištestuoti, dokumentuoti ir autorizuoti. Atsižvelgiant į padarytus pakeitimus ir pastebėtas grėsmes saugumui, testai turėtų būti reguliariai kartojami, testuojant reikėtų įtraukti aktualių ir žinomų galimų atakų scenarijus.

4.6 Reikėtų periodiškai atlikti MPT mokėjimų internetu paslaugų saugumo priemonių auditą, siekiant užtikrinti, kad šios priemonės būtų patikimos ir veiksmingos. Taip pat reikėtų audituoti, kaip įgyvendinamos ir kaip veikia mokėjimų internetu paslaugos. Planuojant šių auditų dažnumą ir turinį, reikėtų atsižvelgti į atitinkamą saugumo riziką, auditas turėtų būti šiai rizikai proporcingas. Auditą turėtų atlikti patikimi ir nepriklausomi (vidaus arba išorės) auditoriai. Jie jokiu būdu neturėtų dalyvauti kuriant, diegiant arba valdant teikiamas mokėjimų internetu paslaugas.

4.7 Jeigu su mokėjimų internetu paslaugų saugumu susijusias funkcijas MPT perduoda vykdyti trečiajai šaliai, į sutartį reikėtų įtraukti nuostatas, pagal kurias būtų reikalaujama laikytis šiose gairėse išdėstytų principų ir rekomendacijų.

4.8 Mokėjimo priemonių priėmimo paslaugą siūlantys MPT pagal sutartį turėtų iš elektroninės prekybos vykdytojų, kurie naudoja (t. y. saugo, tvarko arba perduoda) neskelbtinus mokėjimų duomenis, reikalauti savo IT infrastruktūroje įdiegti 4.1–4.7 gaires atitinkančias saugumo priemones, siekiant išvengti šių neskelbtinų mokėjimų duomenų vagystės per elektroninės prekybos vykdytojų sistemas. Jeigu MPT sužino, kad elektroninės prekybos vykdytojas nėra įdiegęs reikalaujamų apsaugos priemonių, jis turėtų imtis priemonių ir priversti laikytis šios sutartyje nustatytos pareigos arba nutraukti sutartį.

Atsekamumas

5. MPT turėtų būti nustatę tvarką, kuria užtikrintų, kad visos operacijos, taip pat e. įgaliojimų srautas, būtų tinkamai atsekamos.

5.1 MPT turėtų užtikrinti, kad į jų paslaugas būtų įdiegti apsaugos mechanizmai, skirti operacijų ir e. įgaliojimų duomenims, įskaitant operacijos eilės numerį, operacijos laiko įrašus, parametrų pakeitimus ir prieigą prie operacijų ir e. įgaliojimų duomenų, išsamiai registruoti.

5.2 MPT turėtų sudaryti įrašų bylas, kad galėtų atsekti visus atvejus, kai operacijos ir e. įgaliojimų duomenys buvo papildyti, pakeisti arba ištrinti.

5.3 MPT turėtų tikrinti ir analizuoti operacijų ir e. įgaliojimų duomenis ir pasirūpinti priemonėmis šioms įrašų byloms vertinti. Teisė naudotis atitinkamomis taikomosiomis programomis turėtų būti suteikiama tik įgaliotiems darbuotojams.

Specialiosios mokėjimų internetu kontrolės ir saugumo priemonės

Pradinis vartotojo tapatybės nustatymas, vartotojo informavimas

6. Vartotojų tapatybė turėtų būti tinkamai nustatoma laikantis Europos kovos su pinigų plovimu teisės aktų[9], o jų noras atlikti mokėjimus internetu naudojantis paslaugomis turėtų būti patvirtintas prieš suteikiant prieigą prie šių paslaugų. MPT turėtų iš anksto, reguliariai arba, jeigu reikia, *ad hoc* teikti vartotojui informaciją apie būtinus reikalavimus (pavyzdžiui, įrangos, procedūrų), kad mokėjimų internetu operacijos būtų saugios, ir apie šios operacijoms būdingą riziką.

6.1 MPT turėtų užtikrinti, kad būtų atliktos vartotojo išsamaus patikrinimo procedūros, kad vartotojas pateiktų pakankamus tapatybės dokumentus[10] ir su tuo susijusią informaciją, prieš suteikdami vartotojui prieigą prie mokėjimų internetu paslaugų[11].

6.2 MPT turėtų užtikrinti, kad kartu su vartotojui iš anksto pateikiama informacija[12] būtų pateikiami specialieji mokėjimų internetu paslaugų duomenys. Šią informaciją atitinkamai turėtų sudaryti:

- aiški informacija apie visus reikalavimus, taikomus vartotojo įrangai, programinėms arba kitoms reikiamoms priemonėms (pavyzdžiui, antivirusinei programinei įrangai, užkardoms);
- tinkamo ir saugaus asmens duomenų naudojimo gairės;
- nuoseklus tvarkos, kuria vartotojas pateikia mokėjimų operacijos duomenis ir ją autorizuoja ir (arba) gauna informaciją, įskaitant kiekvieno veiksmo padarinius, aprašas;
- tinkamo ir saugaus visos vartotojui suteiktos aparatinės ir programinės įrangos naudojimo gairės;

[9] Pavyzdžiui, 2005 m. spalio 26 d. Europos Parlamento ir Tarybos direktyva 2005/60/EB dėl finansų sistemos apsaugos nuo jos panaudojimo pinigų plovimui ir teroristų finansavimui (OL L 309, 2005 11 25, p. 15–36.) Taip pat žr. 2006 m. rugpjūčio 1 d. Komisijos direktyvą, nustatančią Europos Parlamento ir Tarybos direktyvos 2005/60/EB įgyvendinimo priemones, susijusias su politikoje dalyvaujančių asmenų apibrėžimu, ir supaprastinto deramo klientų tikrinimo procedūroms taikomus techninius kriterijus bei išimtis, suteikiamas dėl to, kad finansine veikla verčiamasi retai arba labai ribotai (OL L 214, 2006 8 4, p. 29–34.).

[10] Pavyzdžiui, pasą, nacionalinę tapatybės kortelę arba saugų elektroninį parašą.

[11] Vartotojo tapatybės nustatymo procesu nepažeidžiamos jokios kovos su pinigų plovimu teisės aktuose nustatytos išimtys. MPT nereikia atskirai nustatyti vartotojo tapatybės tam, kad MPT galėtų suteikti mokėjimo internetu paslaugas, jeigu to vartotojo tapatybę MPT jau nustatė, pavyzdžiui, teikdamas kitas su mokėjimu susijusias paslaugas arba atidarydamas sąskaitą.

[12] Šia informacija papildomi MPD 42 straipsnyje nurodyti duomenys; tame straipsnyje nurodyta, kokią informaciją MPT privalo pateikti mokėjimo paslaugų gavėjui prieš sudarydamas sutartį dėl mokėjimo paslaugų teikimo.

- tvarkos, kurios reikia laikytis, jei parandami arba pavagiami asmens duomenys arba vartotojo aparatinė ar programinė įranga, kuria vartotojas registruojasi arba atlieka operacijas, aprašas;

- tvarkos, kurios reikia laikytis nustačius arba įtarus piktnaudžiavimo atvejį, aprašas;

- atitinkamos MPT ir vartotojo atsakomybės ir įsipareigojimų, susijusių su naudojimusi mokėjimų internetu paslauga, aprašas.

6.3 MPT turėtų užtikrinti, kad bendrojoje sutartyje su vartotoju būtų nurodyta, jog MPT saugumo sumetimais gali užblokuoti konkrečią operaciją arba mokėjimo priemonę[13]. MPT, laikydamasis MPD, turėtų nustatyti vartotojo informavimo metodą, sąlygas ir tai, kaip vartotojas gali kreiptis į MPT, kad mokėjimo internetu operacijos arba paslaugos blokavimas būtų panaikintas.

[13] Žr. MPD 55 straipsnį dėl mokėjimo priemonės naudojimo ribų.

Griežtas vartotojo autentiškumo patvirtinimas

7. Mokėjimų internetu inicijavimas, taip pat prieiga prie neskelbtinų mokėjimo duomenų turėtų būti apsaugoti griežto vartotojo autentiškumo patvirtinimo tvarka. MPT turėtų nustatyti griežto vartotojo autentiškumo patvirtinimo tvarką, laikydamiesi šiose gairėse pateiktos apibrėžties.

7.1 [kredito pervedimas / e. įgaliojimas / e. pinigai] Kad vartotojas galėtų autorizuoti mokėjimų internetu operacijas (įskaitant sugrupuotus kredito pervedimus) ir suteikti arba iš dalies pakeisti elektroninius tiesioginio debeto įgaliojimus, MPT turėtų atlikti griežto vartotojo autentiškumo patvirtinimo procedūrą. Tačiau MPT galėtų svarstyti galimybę taikyti alternatyvias vartotojo autentiškumo patvirtinimo priemones:

- mokėjimams patikimiems gavėjams, įtrauktiems į mokėjimo paslaugų vartotojo nustatytą gavėjų sąrašą;
- operacijoms, kurios atliekamos tarp dviejų to paties vartotojo sąskaitų, atidarytų to paties MPT įstaigoje;
- lėšų pervedimams to paties MPT įstaigoje, pagrįstiems operacijos rizikos analize;
- mažos vertės mokėjimams, nurodytiems MPD[14].

7.2 Norint gauti prieigą prie neskelbtinų mokėjimo duomenų arba šiuos duomenis iš dalies pakeisti (taip pat sudaryti ir iš dalies pakeisti baltuosius sąrašus), reikia atlikti griežto vartotojo autentiškumo patvirtinimo procedūrą. Jeigu MPT teikia vien konsultacines paslaugas, neatskleisdamas neskelbtinos vartotojo arba mokėjimo informacijos, pavyzdžiui, mokėjimo kortelės duomenų, kuriais būtų lengva pasinaudoti neleistiniems tikslams ir sukčiauti, MPT, remdamasis rizikos vertinimu, gali pakoreguoti savo autentiškumo patvirtinimo reikalavimus.

7.3 [kortelės] Operacijų kortelėmis atveju visi korteles išduodantys MPT turėtų turėti galimybę taikyti griežto kortelės turėtojo autentiškumo patvirtinimo priemones. Visos išduotos kortelės privalo būti techniškai parengtos (užregistruotos) naudoti taikant griežto autentiškumo patvirtinimo priemones.

7.4 [kortelės] Mokėjimo priemonių priėmimo paslaugas siūlantys MPT turėtų turėti galimybę naudoti technologijas, kuriomis kortelę išdavęs MPT galėtų atlikti griežto kortelės turėtojo autentiškumo patvirtinimo procedūrą mokėjimų kortele sistemose, kuriose dalyvauja mokėjimo priemones priimantis subjektas.

7.5 [kortelės] Mokėjimo priemonių priėmimo paslaugas siūlantys MPT turėtų iš savo elektroninės prekybos vykdytojo reikalauti užtikrinti galimybę naudoti sprendimus,

[14] Žr. MPD 34 straipsnio 1 dalyje ir 53 straipsnio 1 dalyje pateiktą mažos vertės mokėjimo priemonių apibrėžtį.

kuriais išdavėjas galėtų atlikti griežto kortelės turėtojo autentiškumo patvirtinimo procedūrą, kai operacijos kortele vykdomos internetu. Iš anksto nustatytų kategorijų mažos rizikos operacijoms, pavyzdžiui, remiantis operacijų rizikos analize arba tada, kai atliekami mažos vertės mokėjimai, kaip nurodyta MPD, galima svarstyti galimybę taikyti alternatyvias autentiškumo patvirtinimo priemones.

7.6 [kortelės] Mokėjimų kortele schemose, kurios paslaugai teikti yra priimtinos, skaitmeninės piniginės sprendimų teikėjai turėtų reikalauti iš kortelę išdavusio MPT atlikti griežto autentiškumo patvirtinimo procedūrą, kai teisėtas kortelės turėtojas pirmą kartą užregistruoja kortelės duomenis.

7.7 Skaitmeninės piniginės sprendimų teikėjai turėtų turėti galimybę atlikti griežto autentiškumo patvirtinimo procedūrą, kai vartotojai registruojasi, norėdami naudotis skaitmeninės piniginės mokėjimų paslaugomis, arba atlieka operacijas kortele internete. Iš anksto nustatytų kategorijų mažos rizikos operacijoms, pavyzdžiui, remiantis operacijų rizikos analize arba tada, kai atliekami mažos vertės mokėjimai, kaip nurodyta MPD, galima svarstyti galimybę taikyti alternatyvias autentiškumo patvirtinimo priemones.

7.8 [kortelės] Virtualiųjų kortelių pradinė registracija turėtų vykti saugioje ir patikimoje aplinkoje[15]. Norint generuoti virtualiosios kortelės duomenis, jeigu kortelė išduodama internetinėje aplinkoje, reikėtų atlikti griežto vartotojo autentiškumo patvirtinimo procedūrą.

7.9 MPT turėtų užtikrinti tinkamą dvišalį autentiškumo patvirtinimą, kai palaiko ryšį su elektroninės prekybos vykdytojais ir kai norima inicijuoti mokėjimus internetu bei prieiti prie neskelbtinų mokėjimo duomenų.

Registravimasis autentiškumui patvirtinti ir autentiškumo patvirtinimo priemonių ir (arba) programinės įrangos suteikimas vartotojui

8. MPT turėtų užtikrinti, kad vartotojas galėtų registruotis autentiškumui patvirtinti ir kad vartotojui pirminės autentiškumo patvirtinimo priemonės, kurių reikia norint naudotis mokėjimo internetu paslauga, ir (arba) su mokėjimais susijusi programinė įranga būtų suteikta saugiai.

8.1 Registruojantis autentiškumui patvirtinti ir suteikiant vartotojui autentiškumo patvirtinimo priemones ir (arba) su mokėjimais susijusią programinę įrangą reikėtų laikytis šių reikalavimų.

[15] Aplinka, už kurią yra atsakingi MPT ir kurioje užtikrinamas tinkamas vartotojo ir paslaugą siūlančio MPT autentiškumo patvirtinimas ir konfidencialių ir (arba) neskelbtinų duomenų apsauga, gali būti: i) MPT patalpos; ii) internetinės bankininkystės arba kita saugi interneto svetainė, pavyzdžiui, kurioje svetainę suteikiantis subjektas užtikrina (be kitų dalykų) 4 gairėje nurodytoms priemonėms lygiavertes saugumo funkcijas; iii) bankomatai. (Kai naudojami bankomatai, reikalingas griežtas vartotojo autentiškumo patvirtinimas. Šiam autentiškumui patvirtinti dažniausiai naudojamas lustas ir asmens identifikavimo numeris arba lustas ir biometriniai duomenys.)

- Atitinkamos procedūros turėtų būti atliekamos saugioje ir patikimoje aplinkoje, atsižvelgiant į galimą riziką, kylančią dėl įrenginių, kurių MPT nekontroliuoja.

- Turėtų būti nustatyta veiksminga ir saugi asmens duomenų, su mokėjimais susijusios programinės įrangos ir visų su mokėjimais susijusių pagal asmeninius poreikius pritaikytų įrenginių perdavimo tvarka. Internetu perduodamą programinę įrangą MPT taip pat turėtų patvirtinti elektroniniu parašu, kad vartotojas galėtų patikrinti programinės įrangos autentiškumą ir įsitikinti, jog ji nesuklastota.

- [kortelės] Kai atlieka operacijas kortele, vartotojas turėtų turėti galimybę užsiregistruoti atlikti griežtą autentiškumo patvirtinimą, nesvarbu, ką jis perka internetu. Jeigu perkant internetu siūloma šią paslaugą įjungti, tai turėtų būti padaryta vartotoją nukreipus į saugią ir patikimą aplinką.

8.2 [kortelės] Išdavėjai turėtų aktyviai skatinti kortelės turėtojus registruotis atlikti griežtą autentiškumo patvirtinimą ir leisti savo kortelių turėtojams tuo tikslu nesiregistruoti tik išimtiniais ir tik kai kuriais atvejais, jeigu toks elgesys yra pateisinamas atsižvelgiant į su konkrečia operacija kortele susijusią riziką.

Bandymai prisijungti, seansui skirto laiko pabaiga, autentiškumo patvirtinimo galiojimas

9. MPT turėtų apriboti bandymų prisijungti arba patvirtinti autentiškumą skaičių, apibrėžti mokėjimo internetu paslaugų seansui skirto laiko pabaigos taisykles ir nustatyti autentiškumo patvirtinimo galiojimo terminus.

9.1 Kai MPT autentiškumui patvirtinti naudoja vienkartinį slaptažodį, MPT turėtų užtikrinti, kad tokių slaptažodžių galiojimo trukmė būtų apribota iki trumpiausio būtino laiko.

9.2 MPT turėtų nustatyti didžiausią leidžiamą nepavykusių bandymų prisijungti arba patvirtinti autentiškumą skaičių, kuriam išsekus galimybė naudotis mokėjimo internetu paslauga blokuojama (laikinai arba visam laikui). MPT turėtų būti įdiegę saugią blokuotų mokėjimo internetu paslaugų įjungimo iš naujo procedūrą.

9.3 MPT turėtų nustatyti ilgiausią galimą laiką, kuriam pasibaigus neaktyvūs mokėjimo internetu paslaugų seansai savaime nutraukiami.

Operacijų stebėsena

10. Operacijų stebėsenos mechanizmai, skirti nesąžiningų mokėjimo operacijų prevencijai, nesąžiningoms mokėjimų operacijoms nustatyti ir blokuoti, turėtų imti veikti iki MPT galutinio autentiškumo patvirtinimo; jei operacijos įtartinos arba labai rizikingos, turėtų būti atliekamos specialios tikrinimo ir vertinimo procedūros. Taip pat turėtų būti įdiegti lygiaverčiai e. įgaliojimų išdavimo saugumo stebėsenos ir autorizavimo mechanizmai.

10.1 MPT turėtų naudoti sukčiavimo nustatymo ir prevencijos sistemas ir nustatyti įtartinas operacijas prieš galutinai autorizuodami operacijas arba e. įgaliojimus. Šiose sistemose turėtų būti taikomos, pavyzdžiui, tam tikrais parametrais pagrįstos taisyklės (pavyzdžiui, kortelių duomenų, kurių saugumas buvo pažeistas arba kurie buvo pavogti, juodieji sąrašai), stebima nejprasta vartotojo elgsena arba neįprastas prisijungimas vartotojo prieigos įrenginiu (pavyzdžiui, interneto protokolo (IP) adreso[16] arba IP diapazono pasikeitimas per mokėjimo internetu paslaugų seansą, kartais nustatomas pagal geolokacines IP patikras[17], konkrečiam vartotojui nebūdingos elektroninės prekybos vykdytojų kategorijos arba neįprasti operacijos duomenys ir t. t.). Šiose sistemose taip pat turi būti galima nustatyti kenkimo programinės įrangos naudojimo per seansą požymius (pavyzdžiui, pagal tai, ar patvirtinimą suteikia žmogus, ar patvirtinimas suteikiamas programa) ir žinomus sukčiavimo scenarijus. Stebėsenos sprendimų mastas, sudėtingumas ir pritaikomumas, kartu laikantis atitinkamų duomenų apsaugos teisės aktų, turėtų būti atitikti rizikos vertinimo rezultatus.

10.2 Mokėjimo priemones priimantys MPT turėtų būti įdiegę sukčiavimo nustatymo ir prevencijos sistemas, kuriomis galėtų stebėti elektroninės prekybos vykdytojų veiklą.

10.3 MPT turėtų atlikti visas operacijų tikrinimo ir vertinimo procedūras per reikiamą laiką, kad be reikalo neuždelstų atitinkamos mokėjimo paslaugos inicijavimo ir (arba) vykdymo.

10.4 Jeigu vadovaudamasis savo rizikos politika MPT nusprendžia blokuoti mokėjimo operaciją, kurią įvertino kaip nesąžiningą, MPT turėtų šią operaciją blokuoti kuo trumpiau, kol bus išspręsti saugumo klausimai.

Neskelbtinų mokėjimų duomenų apsauga

11. Neskelbtinus mokėjimo duomenis laikant, tvarkant ir perduodant reikėtų apsaugoti.

11.1 Visi duomenys, kurie naudojami vartotojo autentiškumui nustatyti ir patvirtinti (pavyzdžiui, vartotojui prisijungiant, inicijuojant mokėjimus internetu, suteikiant, iš dalies keičiant arba atšaukiant e. įgaliojimus), taip pat vartotojo sąsajos (MPT arba elektroninės prekybos vykdytojo interneto svetainės) autentiškumui nustatyti ir patvirtinti, turėtų būti tinkamai apsaugoti nuo vagystės ir neteisėtos prieigos arba pakeitimo.

11.2 MPT turėtų užtikrinti, kad besikeisdamos neskelbtinais duomenimis internetu ryšį palaikančios šalys per visą ryšio seansą naudotų saugaus šifravimo galiniuose

[16] IP adresas yra unikalus skaičių kodas, pagal kurį nustatoma kiekvieno prie interneto prijungto kompiuterio tapatybė.

[17] Per geolokacinę IP patikrą tikrinama, ar jį suteikusi valstybė atitinka IP adresą, iš kurio vartotojas inicijuoja operaciją.

įrenginiuose metodus (angl. *end-to end*)[18], kad, naudodamos patikimus ir plačiai pripažintus kodavimo metodus, galėtų išsaugoti duomenų konfidencialumą ir vientisumą.

11.3 Mokėjimo priemonių priėmimo paslaugas siūlantys MPT turėtų skatinti savo elektroninės prekybos vykdytojus nelaikyti jokių neskelbtinų mokėjimo duomenų. Jeigu elektroninės prekybos vykdytojai naudoja, t. y. laiko, tvarko arba perduoda, neskelbtinus mokėjimų duomenis, tokie MPT turėtų pagal sutartį iš elektroninės prekybos vykdytojų reikalauti įdiegti reikiamas šių duomenų apsaugos priemones. MPT turėtų atlikti reguliarias patikras ir, sužinoję, kad neskelbtinus duomenis naudojantis elektroninės prekybos vykdytojas nėra įdiegęs reikalaujamų apsaugos priemonių, imtis priemonių ir priversti laikytis šios sutartyje nustatytos pareigos arba nutraukti sutartį.

[18] Šifravimas galiniuose įrenginiuose – tai duomenų užšifravimas sistemos pradiniame taške ir atitinkamų duomenų iššifravimas tik sistemos paskirties taške. ETSI EN 302 109 V1.1.1. (2003-06).

Vartotojų informavimas, švietimas ir ryšiai su vartotojais

Vartotojų švietimas ir ryšiai su vartotojais

12. Prireikus MPT turėtų teikti vartotojams pagalbą ir rekomendacijas dėl saugaus naudojimosi mokėjimų internetu paslaugomis. MPT turėtų ryšius su savo vartotojais palaikyti taip, kad vartotojas galėtų įsitikinti, jog gautas pranešimas yra autentiškas.

12.1 MPT turėtų suteikti bent vieną apsaugotą kanalą[19] nuolatiniam ryšiui su vartotojais palaikyti tinkamo ir saugaus naudojimosi mokėjimų internetu paslauga klausimais. MPT turėtų informuoti vartotojus apie šį kanalą ir paaiškinti, kad joks MPT vardu kitomis priemonėmis, pavyzdžiui, e. paštu, atsiųstas pranešimas dėl tinkamo ir saugaus naudojimosi mokėjimų internetu paslauga nėra patikimas. MPT turėtų paaiškinti:

- tvarką, kuria vartotojai praneša MPT apie (įtartinus) nesąžiningus mokėjimus, įtartinus incidentus arba neįprastus atvejus, kilusius naudojantis mokėjimų internetu paslaugomis, ir (arba) galimus bandymus pasinaudoti socialinės inžinerijos priemonėmis[20];
- kitus etapus, t. y. tai, kaip MPT atsakys vartotojui;
- tai, kaip MPT praneš vartotojui apie (galimai) nesąžiningas operacijas arba kad operacijos nebuvo inicijuotos, įspės vartotoją apie atakų atvejus (pavyzdžiui, e. pašto duomenų vagystes).

12.2 Apsaugotu kanalu MPT turėtų nuolat informuoti vartotojus apie atnaujintas mokėjimų internetu paslaugų saugumo procedūras. Visi perspėjimai apie kilusią reikšmingą riziką (pavyzdžiui, įspėjimai dėl socialinės inžinerijos) taip pat turėtų būti teikiami apsaugotu kanalu.

12.3 MPT turėtų teikti pagalbą vartotojams visais klausimais, pagal visus skundus, pagalbos prašymus ir pranešimus apie neįprastus naudojimosi mokėjimų internetu paslaugomis ir susijusiomis paslaugomis atvejus arba incidentus; vartotojai turėtų būti tinkamai informuojami, kaip tokią pagalbą gauti.

12.4 MPT turėtų pradėti vykdyti vartotojų švietimo ir informavimo programas, kuriomis užtikrintų, kad vartotojai žinotų, jog turi bent:

- saugoti savo slaptažodžius, prieigos raktus, asmeninius duomenis ir kitus konfidencialius duomenis;

[19] Pavyzdžiui, specialią pašto dėžutę MPT interneto svetainėje arba apsaugotoje svetainėje.

[20] Čia socialine inžinerija vadinami metodai, kuriais manipuliuojama žmonėmis, siekiant gauti informacijos (pavyzdžiui, e. paštu, telefonu), rinkti informaciją socialiniuose tinkluose sukčiavimo tikslais arba įgyti neteisėtą prieigą prie kompiuterio arba tinklo.

- tinkamai valdyti asmeninio įrenginio (pavyzdžiui, kompiuterio) saugumą diegdami ir atnaujindami saugumo priemones (antivirusinę programą, užkardas, saugumo pataisas);

- atsižvelgti į reikšmingas grėsmes ir riziką, susijusią su programinės įrangos parsisiuntimu internetu, jeigu negali būti pagrįstai tikri, kad programinė įranga yra autentiška ir nesuklastota;

- naudoti autentišką MPT mokėjimų internetu paslaugų interneto svetainę.

12.5 Mokėjimo priemones priimantys MPT turėtų iš elektroninės prekybos vykdytojų reikalauti aiškiai atskirti su mokėjimais susijusius procesus nuo internetinės parduotuvės, kad vartotojams būtų lengviau nustatyti, kada jie ryšį palaiko su MPT, o ne su mokėjimo gavėju (pavyzdžiui, nukreipti vartotoją į atvertą atskirą langą, kad mokėjimo procesas būtų rodomas ne elektroninės prekybos vykdytojo lange).

Pranešimai, ribų nustatymas

13. MPT turėtų nustatyti mokėjimų internetu paslaugų ribas ir gali suteikti savo vartotojams galimybes laikantis šių ribų riziką apriboti dar labiau. MPT taip pat gali teikti perspėjimo ir vartotojo profilio valdymo paslaugas.

13.1 Prieš vartotojui teikdamas mokėjimo internetu paslaugas, MPT turėtų nustatyti toms paslaugoms taikomas ribas[21] (pavyzdžiui, didžiausią galimą kiekvieno mokėjimo sumą arba bendrą didžiausią galimą mokėjimo per tam tikrą laikotarpį sumą) ir savo vartotojus atitinkamai informuoti. MPT turėtų leisti vartotojams atsisakyti mokėjimo internetu funkcijos.

Vartotojų prieiga prie informacijos apie mokėjimo inicijavimo ir vykdymo būklę

14. MPT turėtų savo vartotojams patvirtinti, kad mokėjimas inicijuotas, ir laiku suteikti informaciją, kurios reikia norint patikrinti, ar mokėjimo operacija tinkamai inicijuota ir (arba) įvykdyta.

14.1 [kredito pervedimas / e. įgaliojimas] MPT turėtų vartotojams nedelsiant suteikti galimybę, kuria būtų galima bet kuriuo metu[22] saugioje ir patikimoje aplinkoje patikrinti operacijos vykdymo būklę ir sąskaitų likučius.

14.2 Visi išsamūs elektroniniai išrašai turėtų būti pateikiami saugioje ir patikimoje aplinkoje. Kai MPT informuoja vartotojus apie galimybę gauti elektroninius išrašus (pavyzdžiui, reguliariai, kai teikiami periodiniai e. išrašai, arba *ad hoc* išrašus, kai išrašas

[21] Šios ribos gali būti taikomos visuotinai (t. y. visoms mokėjimo priemonėms, kuriomis galima vykdyti mokėjimus internetu) arba konkrečiais atvejais.

[22] Išskyrus išimtinius atvejus, kai priemone negalima naudotis dėl techninės priežiūros arba dėl didelių incidentų.

pateikiamas įvykdžius operaciją) alternatyviu kanalu, pavyzdžiui SMS žinute, e. paštu arba raštu, neskelbtini duomenys į šiuos pranešimus neįtraukiami, o jei įtraukiami – turėtų būti maskuojami.

III dalis. Baigiamosios nuostatos ir įgyvendinimas

15. Šios gairės taikomos nuo 01.08.2015.

1 priedas. Geriausios patirties pavyzdžiai

Be pirmiau išdėstytų reikalavimų, šiose gairėse pateikiama geriausios patirties pavyzdžių, kuriais MPT ir atitinkamiems rinkos dalyviams vadovautis siūloma, bet neprivaloma. Kad būtų suprantamiau, konkrečiai nurodyti skyriai, kuriems taikomi šie geriausios patirties pavyzdžiai.

Bendroji kontrolės ir saugumo aplinka

Valdymas

1 GP pavyzdys. Saugumo politika turėtų būti išdėstyta specialiai tam skirtame dokumente.

Rizikos kontrolė ir mažinimas

2 GP pavyzdys. MPT galėtų suteikti saugias priemones (pavyzdžiui, tinkamai apsaugotus įrenginius ir (arba) vartotojui pritaikytas naršykles), kad vartotojo sąsaja būtų apsaugota nuo neteisėto naudojimo arba atakų (pavyzdžiui, įsilaužimo į naršyklę (angl. *man in the browser)*.

Atsekamumas

3 GP pavyzdys. Mokėjimo priemonių priėmimo paslaugas siūlantys MPT galėtų iš elektroninės prekybos vykdytojų, kurie laiko mokėjimų informaciją, pagal sutartį reikalauti nustatyti reikiamą tvarką, kuria būtų užtikrinta atsekamumo galimybė.

Specialiosios mokėjimų internetu kontrolės ir saugumo priemonės

Pradinis vartotojo tapatybės nustatymas, vartotojo informavimas

4 GP pavyzdys. Vartotojas galėtų pasirašyti specialią paslaugų sutartį dėl mokėjimų internetu operacijų vykdymo, užuot sutikęs šias sąlygas įtraukti į platesnę bendrąją su MPT sudarytą paslaugų sutartį.

5 GP pavyzdys. MPT taip pat galėtų užtikrinti, kad vartotojams būtų reguliariai arba, jei reikia, *ad hoc* ir tinkamomis priemonėmis (pavyzdžiui, lankstinukuose, interneto svetainėse) teikiamos aiškios ir konkrečios instrukcijos, kuriose būtų paaiškinta jų atsakomybė už saugų naudojimąsi šia paslauga.

Griežtas vartotojo autentiškumo patvirtinimas

6 GP pavyzdys. [kortelės] Elektroninės prekybos vykdytojai galėtų užtikrinti galimybę kortelės išdavėjui atlikti griežto kortelių turėtojų autentiškumo patvirtinimo procedūrą per internetu kortelėmis atliekamas operacijas.

7 GP pavyzdys. Kad vartotojams būtų patogiau, MPT galėtų apsvarstyti galimybę naudoti vieną griežto vartotojų autentiškumo patvirtinimo priemonę teikiant visas mokėjimų internetu paslaugas. Šį sprendimą vartotojai labiau pripažintų ir jį būtų lengviau naudoti.

8 GP pavyzdys. Į griežto vartotojų autentiškumo patvirtinimo procedūrą būtų galima įtraukti tam tikrus elementus, kuriais autentiškumo tvirtinimas būtų susietas su konkrečia suma ir mokėjimo gavėju. Taip vartotojams autorizuojant mokėjimą būtų suteikta daugiau tikrumo. Technologinis sprendimas, kuriuo suteikiama galimybė susieti griežto autentiškumo patvirtinimo ir operacijos duomenis, turėtų būti apsaugotas nuo klastojimo.

Neskelbtinų mokėjimų duomenų apsauga

9 GP pavyzdys. Reikėtų, kad neskelbtinus duomenis naudojantys elektroninės prekybos vykdytojai reikiamai išmokytų savo darbuotojus, kurie administruoja sukčiavimo atvejus, ir reguliariai atnaujintų mokymus, kad jų turinys kintančioje saugumo aplinkoje išliktų aktualus.

Vartotojų švietimas ir ryšiai su vartotojais

10 GP pavyzdys. Reikėtų, kad mokėjimo priemonių priėmimo paslaugas siūlantys MPT savo elektroninės prekybos vykdytojams parengtų šviečiamąsias sukčiavimo prevencijos programas.

Pranešimai, ribų nustatymas

11 GP pavyzdys. Laikydamiesi nustatytų ribų MPT galėtų suteikti savo vartotojams priemonę mokėjimų internetu paslaugų riboms valdyti saugioje ir patikimoje aplinkoje.

12 GP pavyzdys. Laikydamiesi savo rizikos valdymo politikos, MPT galėtų įdiegti vartotojų perspėjimo, pavyzdžiui, telefono skambučiu arba SMS žinute, apie įtartinas arba labai rizikingas mokėjimų operacijas funkcijas.

13 GP pavyzdys. MPT galėtų suteikti galimybę vartotojams konkrečiai nurodyti bendras, pagal asmeninius poreikius pritaikytas taisykles – savo elgesio naudojantis mokėjimų internetu ir su tuo susijusiomis paslaugomis parametrus, pavyzdžiui, kad mokėjimus inicijuos tik iš konkrečių valstybių ir kad iš kitur inicijuoti mokėjimai turėtų būti blokuojami arba vartotojai galėtų konkrečius mokėjimų gavėjus įtraukti į baltąjį arba juodąjį sąrašus.