EBA/GL/2021/03

2021 m. birželio 10 d.

Peržiūrėtos gairės

dėl pranešimų apie didelius incidentus pagal MPD2

1. Atitikties ir pranešimų teikimo pareigos

Šių gairių statusas

1. Šiame dokumente išdėstytos pagal EBA reglamento 16 straipsnį parengtos gairės[1]. Pagal EBI reglamento 16 straipsnio 3 dalį kompetentingos institucijos ir finansų įstaigos privalo dėti visas pastangas siekdamos laikytis šių gairių.

2. Gairėse išdėstoma EBI nuomonė dėl tinkamos priežiūros praktikos Europos finansų priežiūros institucijų sistemoje arba dėl to, kaip Sąjungos teisė turėtų būti taikoma tam tikroje srityje. EBI reglamento 4 straipsnio 2 dalyje apibrėžtos kompetentingos institucijos, kurioms taikomos šios gairės, turėtų jų laikytis ir atitinkamai jas įtraukti į savo praktiką (pvz., iš dalies pakeisti savo teisinę sistemą arba priežiūros procesus), įskaitant tuos atvejus, kai gairės yra visų pirma skiriamos įstaigoms.

Pranešimo reikalavimai

3. Pagal EBI reglamento 16 straipsnio 3 dalį kompetentingos institucijos iki (2021.11.07) EBI turi pranešti, ar jos laikosi arba ketina laikytis šių gairių, arba nurodyti nesilaikymo priežastis. Jeigu kompetentingos institucijos iki šio termino nepateikia jokio pranešimo, EBI laiko, kad jos gairių nesilaiko. Pranešimus reikia siųsti užpildžius EBI svetainėje pateiktą formą ir įrašius nuorodą „EBA/GL/2021/03“. Pranešimus turėtų teikti asmenys, turintys reikiamus įgaliojimus pranešti apie gairių laikymąsi savo kompetentingų institucijų vardu. EBI taip pat būtina pranešti apie visus gairių laikymosi pasikeitimus.

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

[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).

2. Dalykas, taikymo sritis ir apibrėžtys

Dalykas

5. Šios gairės parengtos atsižvelgiant į įgaliojimus, suteiktus Europos bankininkystės institucijai (EBI) pagal 2015 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyvos (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 (MPD2), 96 straipsnio 3 dalį.

6. Visų pirma šiose gairėse nurodomi kriterijai, kaip mokėjimo paslaugų teikėjams klasifikuoti didelius operacinius ir saugumo incidentus, ir formatas bei procedūros, kuriuos jie turėtų taikyti, kad, kaip nustatyta MPD2 96 straipsnio 1 dalyje, praneštų apie tokius incidentus buveinės valstybei narei.

7. Be to, šiose gairėse aptariama, kaip šios kompetentingos institucijos turėtų įvertinti incidento aktualumą ir pranešimų apie incidentus duomenis, kuriais pagal MPD2 96 straipsnio 2 dalį jos keičiasi su kitomis vietos institucijomis.

8. Šiose gairėse taip pat aptariama, kaip EBI ir ECB keičiasi aktualiais duomenimis apie pranešimuose nurodytus incidentus, kad būtų skatinamas bendras ir nuoseklus požiūris.

Taikymo sritis

9. Šios gairės taikomos didelių operacinių ar saugumo incidentų klasifikavimui ir pranešimui apie juos pagal MPD2 96 straipsnį.

10. Šios gairės taikomos visiems incidentams, kuriems taikoma didelio operacinio arba saugumo incidento apibrėžtis, apimanti ir išorinius, ir vidinius įvykius, kurie gali būti arba piktavališki, arba atsitiktiniai.

11. Šios gairės taip pat taikomos tais atvejais, kai didelis operacinis ar saugumo incidentas kyla už Sąjungos ribų (pvz., kai incidentas kyla patronuojančioje įmonėje arba patronuojamoje įmonėje, įsteigtoje už Sąjungos ribų) ir turi poveikį mokėjimo paslaugoms, kurias Sąjungoje įsisteigęs mokėjimo paslaugų teikėjas teikia tiesiogiai (su mokėjimu susijusią paslaugą teikia incidentą patyrusi ne Sąjungos įmonė) arba netiesiogiai (dėl incidento kokiu nors kitu būdu sutrinka mokėjimo paslaugų teikėjo gebėjimas toliau vykdyti mokėjimo veiklą).

12. Šios gairės taip pat taikomos, kai įvyksta didelis incidentas, darantis poveikį funkcijoms, kurias mokėjimo paslaugų teikėjai užsisako iš trečiųjų šalių.

Kam skirta

13. Pirmosios gairės (4 skirsnis) skiriamos mokėjimo paslaugų teikėjams, apibrėžtiems MPD2 4 straipsnio 11 punkte ir nurodytiems Reglamento (ES) 1093/2010 4 straipsnio 1 punkte.

14. Antrosios ir trečiosios gairės (5 ir 6 skirsniai) skiriamos kompetentingoms institucijoms, kaip apibrėžta Reglamento (ES) 1093/2010 4 straipsnio 2 punkto i papunktyje.

Apibrėžtys

15. Jeigu nenurodyta kitaip, MPD2 vartojami ir apibrėžti terminai šiose gairėse turi tokią pačią reikšmę. Be to, šiose gairėse vartojamos šios sąvokų apibrėžtys:

Operacinis ar saugumo incidentas	Pavienis įvykis arba tarpusavyje susijusių įvykių grupė, kurių mokėjimo paslaugų teikėjas neplanavo ir kurie turi arba, tikėtina, turės neigiamą poveikį su mokėjimu susijusių paslaugų vientisumui, prieinamumui, konfidencialumui ir (arba) autentiškumui.
Vientisumas	Turto (įskaitant duomenis) tikslumo ir visumos išsaugojimo ypatybė.
Prieinamumas	Su mokėjimu susijusių paslaugų ypatybė, kai jos yra visiškai prieinamos mokėjimo paslaugų vartotojams ir jie gali jomis naudotis mokėjimo paslaugų teikėjo iš anksto nustatytu priimtinu lygmeniu.
Konfidencialumas	Tokia ypatybė, kad informacija nepadaroma prieinama ir neatskleidžiama leidimo neturintiems asmenims, subjektams ar procesams.
Autentiškumas	Tokia ypatybė, kai šaltinis yra tai, kas teigia esąs.
Su mokėjimu susijusios paslaugos	Bet kuri verslo veikla, kaip nurodyta MPD2 4 straipsnio 3 punkte, ir visos reikiamos pagalbinės techninės funkcijos, kad mokėjimo paslaugos būtų tinkamai teikiamos.

3. Įgyvendinimas

Taikymo terminas

16. Šios gairės taikomos nuo 2022 m. sausio 1 d.

Panaikinimas

17. Nuo 2022 m. sausio 1 d. panaikinamos šios gairės:

Gairės dėl pranešimų apie didelius incidentus pagal Direktyvą (ES) 2015/2366 (MPD2) (EBA/GL/2017/10)

4. Mokėjimo paslaugų teikėjams skirtos gairės dėl pranešimo apie didelius operacinius ar saugumo incidentus jų buveinės valstybės narės kompetentingai institucijai

1 gairė. Priskyrimas prie didelių incidentų

1.1. Mokėjimo paslaugų teikėjai dideliems operaciniams ar saugumo incidentams turėtų priskirti tokius incidentus, kurie atitinka:

a. vieną arba daugiau didesnio poveikio lygio kriterijų arba

b. tris arba daugiau mažesnio poveikio lygio kriterijų,

kaip nustatyta 1.4 gairėje, ir tai turėtų daryti vadovaudamiesi šiose gairėse išdėstytu vertinimu.

1.2. Mokėjimo paslaugų teikėjai turėtų įvertinti operacinį ar saugumo incidentą pagal toliau nurodytus kriterijus ir atitinkamus jų rodiklius:

i. Paveiktos operacijos

Mokėjimo paslaugų teikėjai turėtų nustatyti bendrą paveiktų operacijų vertę ir sutrikdytų mokėjimų skaičių, t. y. jų procentinę dalį nuo mokėjimų, atliekamų teikiant paveiktas mokėjimo paslaugas, įprasto skaičiaus.

ii. Paveikti mokėjimo paslaugų vartotojai

Mokėjimo paslaugų teikėjai turėtų nustatyti absoliutų paveiktų mokėjimo paslaugų vartotojų skaičių ir jų procentinę dalį nuo bendro mokėjimo paslaugų vartotojų skaičiaus.

iii. Tinklų ar informacinių sistemų saugumo pažeidimas

Mokėjimo paslaugų teikėjai turėtų nustatyti, ar dėl kokių nors kenkėjiškų veiksmų sumažėjo su mokėjimo paslaugų teikimu susijusio tinklo ar informacinių sistemų saugumas.

iv. Paslaugos nevykdymo laikas

Mokėjimo paslaugų teikėjai turėtų nustatyti laikotarpį, kai paslauga tikriausiai bus neprieinama mokėjimo paslaugų vartotojui arba kai mokėjimo paslaugų teikėjas negalės įvykdyti mokėjimo nurodymo, kaip apibrėžta MPD2 4 straipsnio 13 punkte.

v. Ekonominis poveikis

Mokėjimo paslaugų teikėjai turėtų holistiniu metodu nustatyti su incidentu susijusias pinigines išlaidas, atsižvelgdami ir į absoliutų skaičių, ir, taikytinais atvejais – į santykinę šių išlaidų svarbą, palyginti su mokėjimo paslaugų teikėjo dydžiu (t. y. palyginti su mokėjimo paslaugų teikėjo 1 lygio kapitalu).

vi. Aukšto lygio vidinė sklaida

Mokėjimo paslaugų teikėjai turėtų nustatyti, ar apie šį incidentą buvo arba tikriausiai bus pranešta jų vadovams.

vii. Kiti galbūt paveikti mokėjimo paslaugų teikėjai arba aktualūs infrastruktūros objektai

Mokėjimo paslaugų teikėjai turėtų nustatyti sisteminius padarinius, kuriuos tikriausiai turės incidentas, t. y. tikimybę, kad šie padariniai bus jaučiami už pradinio paveikto mokėjimo paslaugų teikėjo ribų kitiems mokėjimo paslaugų teikėjams, finansų rinkos infrastruktūros objektams ir (arba) mokėjimo sistemoms.

viii. Poveikis reputacijai

Mokėjimo paslaugų teikėjai turėtų nustatyti, kaip incidentas gali sumenkinti vartotojų pasitikėjimą pačiu mokėjimo paslaugų teikėju ir apskritai atitinkama paslauga arba visa rinka.

1.3. Rodiklių vertę mokėjimo paslaugų teikėjai turėtų apskaičiuoti pagal toliau nurodytą metodiką.

i. Paveiktos operacijos:

Paprastai mokėjimo paslaugų teikėjai paveiktomis operacijomis turėtų laikyti visas šalies vidaus ar tarpvalstybines operacijas, kurioms incidentas turėjo arba tikriausiai turės tiesioginį arba netiesioginį poveikį, ir ypač tas operacijas, kurių nebuvo įmanoma inicijuoti arba apdoroti, taip pat tas operacijas, kurių mokėjimo paskirties turinys buvo pakeistas, ir tas, kurias buvo pavesta atlikti apgaule (nesvarbu, ar lėšos buvo susigrąžintos, ar ne), arba kai dėl incidento užkertamas kelias ar kokiu nors kitu būdu trukdoma tinkamai vykdyti operacijas.

Operacinių incidentų atveju, kai padaromas poveikis gebėjimui inicijuoti ir (arba) apdoroti sandorius, mokėjimo paslaugų teikėjai turėtų pranešti tik apie incidentus, trunkančius ilgiau nei vieną valandą. Incidento trukmė turėtų būti matuojama nuo momento, kada incidentas įvyksta, iki momento, kada įprasta veikla / operacijos atsigavo iki tokio paslaugų lygio, koks buvo prieš incidentą.

Be to, mokėjimo paslaugų teikėjai įprastu mokėjimo operacijų lygiu turėtų laikyti šalies vidaus ir tarpvalstybinių mokėjimo operacijų, atliekamų teikiant incidento paveiktas mokėjimo paslaugas, kasdienį metinį vidurkį, o apskaičiavimų atskaitos laikotarpiu laikyti praėjusius metus. Jeigu mokėjimo paslaugų teikėjai šio skaičiaus nelaiko reprezentatyviu (pvz., dėl sezoniškumo), jie turėtų naudoti kitą, reprezentatyvesnį rodiklį ir atitinkamame šablono laukelyje (žr. priedą) kompetentingai institucijai nurodyti atitinkamą šio metodo loginį pagrindą.

ii. Paveikti mokėjimo paslaugų vartotojai

Paveiktais mokėjimo paslaugų vartotojais mokėjimo paslaugų teikėjai turėtų laikyti visus klientus (tiek šalies vidaus klientus, tiek klientus iš užsienio, tiek vartotojus, tiek įmones), turinčius sutartį su paveiktu mokėjimo paslaugų teikėju, pagal kurią jiems suteikiama teisė naudotis paveikta mokėjimo paslauga, ir patyrusius arba tikriausiai patirsiančius incidento padarinių. Remdamiesi ankstesne veikla, mokėjimo paslaugų teikėjai turėtų atlikti apytikrius vertinimus, kad galėtų nustatyti, kiek mokėjimo paslaugų vartotojų galėjo naudotis mokėjimo paslauga incidento aktualumo laikotarpiu.

Grupių atveju kiekvienas mokėjimo paslaugų teikėjas turėtų atsižvelgti tik į savo mokėjimo paslaugų vartotojus. Kai mokėjimo paslaugų teikėjas teikia veiklos paslaugas kitiems, tas mokėjimo paslaugų teikėjas turėtų atsižvelgti tik į savo mokėjimo paslaugų vartotojus (jeigu jų yra), o tas veiklos paslaugas gaunantys mokėjimo paslaugų teikėjai turėtų įvertinti incidentą atsižvelgdami į savo pačių mokėjimo paslaugų vartotojus.

Operacinių incidentų atveju, kai padaromas poveikis gebėjimui inicijuoti ir (arba) apdoroti sandorius, mokėjimo paslaugų teikėjai turėtų pranešti tik apie poveikį mokėjimo paslaugų vartotojams darančius incidentus, trunkančius ilgiau nei vieną valandą. Incidento trukmė turėtų būti matuojama nuo momento, kada incidentas įvyksta, iki momento, kada įprasta veikla / operacijos atsigavo iki tokio paslaugų lygio, koks buvo prieš incidentą.

Be to, mokėjimo paslaugų teikėjai bendru mokėjimo paslaugų vartotojų skaičiumi turėtų laikyti bendrą šalies vidaus ir tarpvalstybinių mokėjimo paslaugų vartotojų, kurie incidento metu (arba pagal naujausius turimus duomenis) su jais turi sutartis ir turi teisę naudotis paveikta mokėjimo paslauga, skaičių, neatsižvelgdami į vartotojų dydį ir į tai, ar jie laikomi aktyviais, ar pasyviais mokėjimo paslaugų vartotojais.

iii. Tinklų ar informacinių sistemų saugumo pažeidimas

Mokėjimo paslaugų teikėjai turėtų nustatyti, ar dėl kokių nors kenkėjiškų veiksmų sumažėjo su mokėjimo paslaugų teikimu susijusio tinklo ar informacinių sistemų (įskaitant duomenis) prieinamumas, autentiškumas, vientisumas arba konfidencialumas.

iv. Paslaugos nevykdymo laikas

Mokėjimo paslaugų teikėjai turėtų apsvarstyti laikotarpį, kurį neveikia arba, tikėtina, neveiks bet kuri su mokėjimo paslaugų teikimu susijusi funkcija, procesas arba kanalas ir dėl to neįmanoma arba nebus įmanoma i) inicijuoti ir (arba) įvykdyti mokėjimo paslaugos ir (arba) ii) prisijungti prie mokėjimo sąskaitos. Paslaugos nevykdymo laiką mokėjimo paslaugų teikėjai turėtų skaičiuoti nuo neveikimo pradžios ir, kai tai aktualu ir taikytina, turėtų atsižvelgti į savo darbo laiko intervalus, reikalingus mokėjimo paslaugoms įvykdyti, taip pat į nedarbo laiką bei techninės priežiūros laikotarpius. Jeigu mokėjimo paslaugų teikėjai negali nustatyti, kada nustojo būti vykdoma paslauga, paslaugos nevykdymo laiką išimties tvarka jie turėtų pradėti skaičiuoti nuo neveikimo aptikimo momento.

v. *Ekonominis poveikis*

Mokėjimo paslaugų teikėjai turėtų atsižvelgti į išlaidas, kurias galima tiesiogiai susieti su incidentu, ir į išlaidas, kurios su incidentu susijusios netiesiogiai. Be kita ko, mokėjimo paslaugų teikėjai turėtų atsižvelgti į nusavintas lėšas ar turtą, aparatinės ar programinės įrangos pakeitimo išlaidas, kitas teismo ar žalos atitaisymo išlaidas, mokesčius, mokėtinus dėl sutartinių prievolių nesilaikymo, sankcijas, išorės įsipareigojimus ir prarastas pajamas. Kalbant apie netiesiogines išlaidas, mokėjimo paslaugų teikėjai turėtų atsižvelgti tik į tas išlaidas, kurios jau yra žinomos arba labai tikėtina, kad jos atsiras.

vi. *Aukšto lygio vidinė sklaida*

Mokėjimo paslaugų teikėjai turėtų apsvarstyti, ar dėl poveikio su mokėjimu susijusioms paslaugoms valdymo organas, kaip apibrėžta EBI IRT ir saugumo rizikos valdymo gairėse, pagal EBI IRT ir saugumo rizikos valdymo gairių 60 gairės d punktą buvo ar tikriausiai bus informuotas apie incidentą nesilaikant jokios periodinių pranešimų teikimo procedūros ir nuolat per visą incidento trukmę. Be to, mokėjimo paslaugų teikėjai turėtų apsvarstyti, ar dėl incidento poveikio su mokėjimu susijusioms paslaugoms yra arba bus pradėta dirbti krizės režimu.

vii. *Kiti galbūt paveikti mokėjimo paslaugų teikėjai arba aktualūs infrastruktūros objektai*

Mokėjimo paslaugų teikėjai turėtų įvertinti incidento poveikį finansų rinkai, kuri suprantama kaip finansų rinkos infrastruktūros objektai ir (arba) mokėjimo sistemos, kuriomis jie remiasi, taip pat likę mokėjimo paslaugų teikėjai. Visų pirma mokėjimo paslaugų teikėjai turėtų įvertinti, ar incidentas pasikartojo arba, tikėtina, pasikartos kitų mokėjimo paslaugų teikėjų praktikoje, taip pat ar jis turėjo arba, tikėtina, turės poveikį sklandžiam finansų rinkos infrastruktūros objektų veikimui ir ar jis pakenkė arba, tikėtina, pakenks patikimam visos finansų sistemos veikimui. Mokėjimo paslaugų teikėjai turėtų nepamiršti įvairių aspektų, pvz., ar paveiktas elementas ir (arba) programinė įranga yra nuosavybinė, ar visuotinai prieinama, ar sutrikdytas tinklas yra vidinis, ar išorinis, ir ar mokėjimo pasaugų teikėjas nutraukė arba, tikėtina, nutrauks savo prievolių vykdymą finansų rinkos infrastruktūros objektuose, kurių narys jis yra.

viii. *Poveikis reputacijai*

Mokėjimo paslaugų teikėjai turėtų atsižvelgti į esamą arba, tikėtina, būsimą incidento matomumą rinkoje. Visų pirma mokėjimo paslaugų teikėjai turėtų apsvarstyti tikimybę, kad incidentas padarys žalą visuomenei – patikimą rodiklį, kad incidentas gali turėti poveikį jų reputacijai. Mokėjimo paslaugų teikėjai turėtų atsižvelgti į tai, ar i) mokėjimo paslaugų vartotojai ir (arba) kiti mokėjimo paslaugų teikėjai skundėsi dėl neigiamo incidento poveikio, ii) incidentas padarė poveikį matomam su mokėjimo paslauga susijusiam procesui ir todėl apie jį tikriausiai praneš arba jau pranešė žiniasklaida (ne tik tokia tradicinė žiniasklaida, kaip laikraščiai, bet ir tinklaraščiai, socialiniai tinklai ir kt.), iii) nebuvo ar tikriausiai nebus įvykdyti sutartiniai įsipareigojimai, tad mokėjimo paslaugų teikėjui bus pareikšta ieškinių, iv) nesilaikoma reguliuojamųjų reikalavimų ir dėl to taikomos priežiūros priemonės ar

sankcijos, kurios buvo ar tikriausiai bus paskelbtos viešai, ir v) panašios rūšies incidentų jau buvę anksčiau.

1.4. Mokėjimo paslaugų teikėjai turėtų įvertinti incidentą pagal kiekvieną atskirą kriterijų nustatydami, ar iki incidento panaikinimo yra arba bus pasiektos 1 lentelėje nurodytos aktualios ribos.

1 lentelė. Ribinės vertės

Kriterijai	Mažesnis poveikio lygis	Didesnis poveikio lygis
Paveiktos operacijos	> 10 proc. mokėjimo paslaugų teikėjo įprasto operacijų lygio (pagal operacijų skaičių) **ir** incidento trukmė > 1 valanda* **arba** > 500 000 EUR **ir** incidento trukmė > 1 valanda*	> 25 proc. mokėjimo paslaugų teikėjo įprasto operacijų lygio (pagal operacijų skaičių) **arba** > 15 000 000 EUR
Paveikti mokėjimo paslaugų vartotojai	> 5 000 **ir** incidento trukmė > 1 valanda* **arba** > 10 proc. mokėjimo paslaugų teikėjo mokėjimo paslaugų vartotojų **ir** incidento trukmė > 1 valanda*	> 50 000 **arba** > 25 proc. mokėjimo paslaugų teikėjo mokėjimo paslaugų vartotojų
Paslaugos nevykdymo laikas	> 2 valandos	Netaikoma
Tinklų ir informacinių sistemų saugumo pažeidimas	Taip	Netaikoma
Ekonominis poveikis	Netaikoma	> Maks. (0,1 proc. 1 lygio kapitalas**, 200 000 EUR) **arba** > 5 000 000 EUR
Aukšto lygio vidinė sklaida	Taip	Taip, ir tikriausiai bus pradėta dirbti kriziniu (arba lygiaverčiu) režimu
Kiti galbūt paveikti mokėjimo paslaugų teikėjai arba aktualūs infrastruktūros objektai	Taip	Netaikoma
Poveikis reputacijai	Taip	Netaikoma

* Ribinė vertė, susijusi su incidento trukme, viršijančia vieną valandą, taikoma tik operaciniams incidentams, darantiems poveikį mokėjimo paslaugų teikėjo gebėjimui inicijuoti ir (arba) apdoroti sandorius.

**1 lygio kapitalas, kaip apibrėžta 2013 m. birželio 26 d. Europos Parlamento ir Tarybos reglamento (ES) Nr. 575/2013 dėl prudencinių reikalavimų kredito įstaigoms ir investicinėms įmonėms ir kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 648/2012, 25 straipsnyje.

1.5. Jeigu mokėjimo paslaugų teikėjai neturi faktinių duomenų, kuriais galėtų pagrįsti savo vertinimą, ar konkreti riba yra arba, tikėtina, bus pasiekta iki incidento panaikinimo, jie turėtų remtis apytikriais vertinimais (pvz., tai galėtų būti padaryta pradinio tyrimo etapu).

1.6. Mokėjimo paslaugų teikėjai incidento aktualumo laikotarpiu šį vertinimą turėtų atlikti nuolat, kad nustatytų galimą būklės pokytį blogėjimo (nuo nedidelio iki didelio incidento) arba gerėjimo (nuo didelio iki nedidelio incidento) linkme. Apie visus atvejus, kai didelis incidentas priskiriamas prie nedidelių incidentų, reikėtų nedelsiant pranešti kompetentingai institucijai pagal 2.21 gairės reikalavimą.

2 gairė. Pranešimo procesas

2.1. Mokėjimo paslaugų teikėjai turėtų rinkti visą aktualią informaciją, užpildydami priede pateiktą šabloną parengti pranešimą apie incidentą ir jį pateikti buveinės valstybės narės kompetentingai institucijai. Mokėjimo paslaugų teikėjai turėtų užpildyti visus šablono laukus, vadovaudamiesi priede pateiktais nurodymais.

2.2. Mokėjimo paslaugų teikėjai turėtų naudoti tą patį šabloną pradiniam, tarpiniam ir galutiniam su tuo pačiu incidentu susijusiam pranešimui pateikti. Todėl mokėjimo paslaugų teikėjai turėtų laipsniškai pildyti vieną šabloną ir, kai taikytina, atnaujinti ankstesniuose pranešimuose pateiktą informaciją.

2.3. Mokėjimo paslaugų teikėjai savo buveinės valstybės narės kompetentingai institucijai, jei taikytina, taip pat turėtų pristatyti savo vartotojams pateiktos informacijos kopiją, kaip nustatyta MPD2 96 straipsnio 1 dalies antroje pastraipoje, kai tik su ja bus galima susipažinti.

2.4. Buveinės valstybės narės kompetentingos institucijos prašymu mokėjimo paslaugų teikėjas turėtų pateikti visus papildomus dokumentus, kuriais papildoma standartiniame šablone pateikta informacija. Mokėjimo paslaugų teikėjai turėtų vykdyti bet kokius buveinės valstybės narės kompetentingos institucijos prašymus pateikti papildomą informaciją ar paaiškinimus dėl jau pateiktos dokumentacijos.

2.5. Mokėjimo paslaugų teikėjas bet kokią papildomą informaciją, esančią mokėjimo paslaugų teikėjų kompetentingai institucijai pateiktuose dokumentuose, mokėjimo paslaugų teikėjo iniciatyva arba kompetentingos institucijos prašymu pagal 2.4 gairę turėtų perteikti šablone pagal 2.1 gairę.

2.6. Mokėjimo paslaugų teikėjai turėtų visą laiką saugoti informacijos, kuria keičiamasi su jų buveinės valstybės narės kompetentinga institucija, konfidencialumą ir vientisumą ir savo buveinės valstybės narės kompetentingai institucijai tinkamai įrodyti savo tapatybę.

Pradinis pranešimas

2.7. Mokėjimo paslaugų teikėjai buveinės valstybės narės kompetentingai institucijai turėtų pateikti pradinį pranešimą, kai operacinis ar saugumo incidentas pripažintas dideliu. Kompetentingos institucijos turėtų nepagrįstai nedelsdamos patvirtinti pradinio pranešimo gavimą ir priskirti incidentui unikalų referencinį kodą, kuriuo jis būtų nedviprasmiškai identifikuojamas. Mokėjimo paslaugų teikėjai turėtų nurodyti šį referencinį kodą, kai pateikia atnaujintą pradinį pranešimą arba atnaujintus tarpinį ir galutinį pranešimus, susijusius su tuo pačiu incidentu, nebent tarpinis ir galutinis pranešimai būtų pateikiami kartu su pradiniu pranešimu.

2.8. Mokėjimo paslaugų teikėjai kompetentingai institucijai turėtų pateikti pradinį pranešimą per keturias valandas nuo to momento, kada operacinis ar saugumo incidentas pripažintas dideliu. Jeigu žinoma, kad kompetentingos institucijos pranešimo kanalai tuo metu neprieinami arba neveikia, mokėjimo paslaugų teikėjai turėtų pateikti pradinį pranešimą tada, kai jie vėl taps prieinami ir (arba) pradės veikti.

2.9. Nustatę incidentą, bet ne vėliau kaip po 24 valandų po incidento nustatymo mokėjimo paslaugų teikėjai turėtų laiku klasifikuoti incidentą pagal 1.1 ir 1.4 gaires ir nepagrįstai nedelsdami, kai tik mokėjimo paslaugų teikėjas turės incidentui klasifikuoti reikalingą informaciją. Jeigu incidentui klasifikuoti reikia daugiau laiko, mokėjimo paslaugų teikėjai kompetentingai institucijai pateiktame pradiniame pranešime turėtų paaiškinti priežastis.

2.10. Mokėjimo paslaugų teikėjai buveinės valstybės narės kompetentingai institucijai taip pat turėtų pateikti pradinį pranešimą, kai anksčiau aptiktas nedidelis incidentas pripažįstamas dideliu incidentu. Šiuo konkrečiu atveju mokėjimo paslaugų teikėjai kompetentingai institucijai turėtų nusiųsti pradinį pranešimą iš karto po būklės pakitimo nustatymo arba, jeigu žinoma, kad tuo metu kompetentingos institucijos pranešimų priėmimo kanalai neprieinami arba neveikia – tada, kai jie vėl taps prieinami ir (arba) pradės veikti.

2.11. Mokėjimo paslaugų teikėjai savo pradiniuose pranešimuose (t. y. šablono A skirsnyje) turėtų pateikti antraščių lygio informaciją, taip apibūdindami kai kurias pagrindines incidento savybes ir numatomus jo padarinius, grindžiamus informacija, kuri tapo prieinama iš karto po to, kai incidentas buvo pripažintas dideliu. Kai faktinių duomenų nėra, mokėjimo paslaugų teikėjai turėtų remtis apytikriais vertinimais.

Tarpinis pranešimas

2.12. Mokėjimo paslaugų teikėjai turėtų pateikti tarpinį pranešimą, kai bus atnaujinta įprasta veikla ir bus sugrįžta prie įprastos verslo eigos, apie šią aplinkybę informuodami kompetentingą instituciją. Mokėjimo paslaugų teikėjai grįžimu prie įprastos verslo eigos turėtų laikyti momentą, kai veikla ir (arba) operacijos atkuriamos iki tokio paties paslaugų ir (arba) sąlygų lygio, kokį mokėjimo paslaugų teikėjas yra apibrėžęs arba koks yra išoriškai nustatytas paslaugų lygmens susitarime – t. y. iki atitinkamo apdorojimo laiko, pajėgumo, saugumo

reikalavimų ir kt., o nenumatytų atvejų priemonės nebetaikomos. Tarpiniame pranešime turėtų būti pateiktas išsamesnis incidento ir jo padarinių aprašymas (šablono B skirsnyje).

2.13. Jeigu įprasta veikla dar neatnaujinta, mokėjimo paslaugų teikėjai turėtų pateikti kompetentingai institucijai tarpinį pranešimą per tris darbo dienas nuo pradinio pranešimo pateikimo.

2.14. Mokėjimo paslaugų teikėjai atnaujinti šablono A ir B skirsniuose jau pateiktą informaciją bent jau tada, kai jie sužino apie didelius pokyčius nuo ankstesniojo pranešimo (pvz., ar incidentas išplito, ar sumažėjo, kokios nustatytos naujos jo priežastys arba kokių veiksmų imtasi problemai išspręsti). Tai apima atvejį, kai incidentas nėra išspręstas per tris darbo dienas ir tokiu atveju mokėjimo paslaugų teikėjai turėtų pateikti papildomą tarpinį pranešimą. Bet kuriuo atveju buveinės valstybės narės kompetentingos institucijos prašymu mokėjimo paslaugų teikėjai turėtų pateikti papildomą tarpinį pranešimą.

2.15. Kaip ir pradinių pranešimų atveju, kai faktinių duomenų nėra, mokėjimo paslaugų teikėjai turėtų atlikti apytikrius vertinimus.

2.16. Jeigu nuo incidento pripažinimo dideliu nepraėjus 4 valandoms būtų sugrįžta prie įprastos verslo eigos, mokėjimo paslaugų teikėjai turėtų siekti iki 4 valandų termino pabaigos vienu metu pateikti ir pradinį, ir tarpinį pranešimą (t. y. užpildyti šablono A ir B skirsnius).

Galutinis pranešimas

2.17. Mokėjimo paslaugų teikėjai turėtų pateikti galutinį pranešimą, kai atliekama pagrindinių priežasčių analizė (neatsižvelgiant į tai, ar poveikio mažinimo priemonės jau įgyvendintos ir ar nustatyta galutinė pagrindinė priežastis) ir turima faktinių duomenų, kuriais būtų galima pakeisti visus galimus įverčius.

2.18. Mokėjimo paslaugų teikėjai daugiausia per 20 darbo dienų nuo grįžimo prie įprastos verslo eigos kompetentingai institucijai turėtų pristatyti galutinį pranešimą. Mokėjimo paslaugų teikėjai, kuriems reikia, kad šis terminas būtų pratęstas (pvz., kai dar nėra faktinių duomenų apie poveikį arba dar nėra nustatytos pagrindinės priežastys), iki termino pabaigos turėtų susisiekti su kompetentinga institucija ir pateikti tinkamą vėlavimo pagrindimą ir naują planuojamą galutinio pranešimo datą.

2.19. Jeigu mokėjimo paslaugų teikėjai visą galutiniam pranešimui reikalingą (t. y. šablono C skirsnio) informaciją gali pateikti per 4 valandų laikotarpį nuo incidento pripažinimo dideliu, jie turėtų siekti savo pradiniame pranešime pateikti informaciją, susijusią su pradiniu, tarpiniu ir galutiniu pranešimais.

2.20. Mokėjimo paslaugų teikėjai turėtų siekti į savo galutinį pranešimą įtraukti visą informaciją, t. y. i) faktinius duomenis apie poveikį, o ne įverčius (taip pat visą kitą atnaujintą informaciją, reikalingą šablono A ir B skirsniuose) ir ii) šablono C skirsnį, kuriame, jeigu jau žinoma,

nurodoma pagrindinė priežastis, jeigu ji jau žinoma, ir apibendrinamos priemonės, kurių buvo imtasi arba planuojama imtis problemai pašalinti ir užtikrinti, kad ji nepasikartotų ateityje.

2.21. Mokėjimo paslaugų teikėjai taip pat turėtų nusiųsti galutinį pranešimą, kai, nuolat analizuodami incidentą, jie nustato, kad incidentas, apie kurį jau pranešta, nebeatitinka kriterijų, pagal kurį jis būtų laikomas dideliu, ir tikimasi, kad iki incidento panaikinimo jis tų kriterijų nebeatitiks. Šiuo atveju mokėjimo paslaugų teikėjai turėtų nusiųsti galutinį pranešimą, kai tik nustatoma ši aplinkybė ir bet kuriuo atveju iki planuojamos kito pranešimo datos. Šiuo konkrečiu atveju mokėjimo paslaugų teikėjai turėtų ne pildyti šablono C skirsnį, o pažymėti langelį *incidentas perklasifikuotas kaip nedidelis* ir paaiškinti šio perklasifikavimo motyvus.

3 gairė. Deleguotasis ir konsoliduotasis pranešimų teikimas

3.1. Leidus kompetentingai institucijai, mokėjimo paslaugų teikėjai, pageidaujantys MPD2 nustatytus pranešimų teikimo įpareigojimus deleguoti trečiajai šaliai, turėtų informuoti buveinės valstybės narės kompetentingą instituciją ir užtikrinti, kad būtų įvykdytos toliau nurodytos sąlygos.

a. Mokėjimo paslaugų teikėjo ir trečiosios šalies oficialia sutartimi arba, kai taikytina, galiojančiais vidaus susitarimais grupėje, kuriais grindžiamas deleguotasis pranešimų teikimas, vienareikšmiškai apibrėžiamas visų šalių pareigų paskirstymas. Visų pirma juose aiškiai nurodoma, kad, nepaisant galimo pranešimų teikimo įpareigojimų delegavimo, paveiktas mokėjimo paslaugų teikėjas lieka visiškai atsakingas ir atskaitingas už MPD2 96 straipsnyje išdėstytų reikalavimų įvykdymą ir už buveinės valstybės narės kompetentingai institucijai teikiamos informacijos turinį.

b. Delegavimas atitinka svarbių veiklos funkcijų perdavimo išorės subjektui reikalavimus, išdėstytus

   i. MPD2 19 straipsnio 6 dalyje dėl mokėjimo įstaigų ir e. pinigų įstaigų, taikomoje *mutatis mutandis* pagal Direktyvos 2009/110/EB 3 straipsnį, arba

   ii. EBI gairėse dėl užsakomųjų paslaugų (EBA/GL/2019/02), susijusius su visais mokėjimo paslaugų teikėjais.

c. Informacija buveinės valstybės narės kompetentingai institucijai teikiama iš anksto ir bet kuriuo atveju laikantis kompetentingos institucijos nustatytų terminų ir procedūrų, kai jos taikomos.

d. Tinkamai užtikrinamas neskelbtinų duomenų konfidencialumas ir kompetentingai institucijai teiktinos informacijos kokybė, nuoseklumas, vientisumas ir patikimumas.

3.2. Mokėjimo paslaugų teikėjai, pageidaujantys leisti paskirtajai trečiajai šaliai konsoliduotai vykdyti pranešimų teikimo įpareigojimus (pvz., teikiant vieną pranešimą, kuriame nurodomi keli to paties didelio operacinio ar saugumo incidento paveikti mokėjimo paslaugų teikėjai), turėtų informuoti buveinės valstybės narės kompetentingą instituciją, pateikti šablono skirsnyje *Paveikti mokėjimo paslaugų teikėjai* nurodomą informaciją ir užtikrinti, kad būtų patenkintos šios sąlygos:

a. įtraukti šią nuostatą į sutartį, kuria grindžiamas deleguotasis pranešimų teikimas;

b. teikti konsoliduotuosius pranešimus, tik jeigu incidentas kilo dėl trečiosios šalies teikiamų paslaugų sutrikimo;

c. konsoliduotąjį pranešimų teikimą taikyti tik toje pačioje valstybėje narėje įsteigtiems mokėjimo paslaugų teikėjams;

d. pateikti visų mokėjimo paslaugų teikėjų, kuriuos paveikė incidentas, sąrašą;

e. užtikrinti, kad trečioji šalis įvertintų incidento reikšmingumą kiekvienam paveiktam mokėjimo paslaugų teikėjui, ir į konsoliduotąjį pranešimą įtraukti tik tuos mokėjimo paslaugų teikėjus, kurių atžvilgiu incidentas pripažintas dideliu; be to, užtikrinti, kad, kai abejojama, mokėjimo paslaugų teikėjas būtų įtrauktas į konsoliduotąjį pranešimą, jeigu nėra priešingų įrodymų;

f. užtikrinti, kad, kai esama šablono laukelių, kuriuose negalima pateikti bendro atsakymo (pvz., B 2, B 4 ar C 3 skirsniuose), trečioji šalis arba i) užpildytų juos kiekvieno paveikto mokėjimo paslaugų teikėjo vardu, toliau nurodydama kiekvieno mokėjimo paslaugų teikėjo, su kuriuo susijusi informacija, tapatybę, arba ii) naudotų bendras vertes, pastebėtas ar apytiksliai įvertintas mokėjimo paslaugų teikėjų atžvilgiu;

g. trečioji šalis visą laiką informuotų mokėjimo paslaugų teikėją apie visus aktualius incidento aspektus ir apie visą galimą trečiosios šalies bendravimą su kompetentinga institucija ir jo turinį, tačiau tik tiek, kiek įmanoma, kad nebūtų pažeistas su kitais mokėjimo paslaugų teikėjais susijusios informacijos konfidencialumas.

3.3. Mokėjimo paslaugų teikėjai neturėtų deleguoti savo pranešimų teikimo įpareigojimų, kol apie tai neinformavo buveinės valstybės narės kompetentingos institucijos, arba jeigu jie gavo informaciją, kad funkcijų perdavimo išorės subjektams susitarimas neatitinka 3.1 gairės b punkte nurodytų reikalavimų.

3.4. Mokėjimo paslaugų teikėjai, pageidaujantys atšaukti savo pranešimų teikimo įpareigojimų delegavimą, turėtų apie šį sprendimą pranešti buveinės valstybės narės kompetentingai institucijai, laikydamiesi pastarosios nustatytų terminų ir procedūrų. Mokėjimo paslaugų teikėjai taip pat turėtų informuoti buveinės valstybės narės kompetentingą instituciją apie

bet kokius svarbius įvykius, turinčius poveikį paskirtajai trečiajai šaliai ir jos gebėjimui įvykdyti pranešimų teikimo įpareigojimus.

3.5. Mokėjimo paslaugų teikėjai turėtų iš esmės įvykdyti savo pranešimų teikimo įpareigojimus nesinaudodami išorės pagalba, jeigu paskirtoji trečioji šalis buveinės valstybės narės kompetentingos institucijos neinformuotų apie didelį operacinį ar saugumo incidentą taip, kaip nurodyta MPD2 96 straipsnyje ir šiose gairėse. Mokėjimo paslaugų teikėjai taip pat turėtų užtikrinti, kad apie incidentą nebūtų pranešama du kartus – kad apie jį atskirai nepraneštų minėtasis mokėjimo paslaugų teikėjas ir dar kartą trečioji šalis.

3.6. Mokėjimo paslaugų teikėjai turėtų užtikrinti, kad tuo atveju, kai incidentą sukėlė techninių paslaugų teikėjo teikiamų paslaugų (ar infrastruktūros) sutrikimas, darantis poveikį daugeliui MPT, deleguojamas pranešimų teikimas būtų susijęs su individualiais mokėjimo paslaugų teikėjo duomenimis (išskyrus konsoliduotuosius pranešimus).

4 gairė. Operacinė ir saugumo politika

4.1. Mokėjimo paslaugų teikėjai turėtų užtikrinti, kad jų bendroje operacinėje ir saugumo politikoje būtų aiškiai apibrėžtos visos pareigos pranešti apie incidentus pagal MPD2 ir būtų įgyvendinti procesai šiose gairėse apibrėžtiems reikalavimams įvykdyti.

5. Kompetentingoms institucijoms skirtos gairės dėl kriterijų, kaip įvertinti incidento aktualumą, ir dėl pranešimų apie incidentus duomenų, kuriais keičiamasi su kitomis vietos institucijomis

5 gairė. Incidento aktualumo įvertinimas

5.1. Buveinės valstybės narės kompetentingos institucijos turėtų įvertinti didelio operacinio ar saugumo incidento aktualumą kitoms vietos institucijoms, kaip pagrindu vadovaudamosi savo pačių ekspertų nuomone ir kaip pagrindinius minėtojo incidento svarbos rodiklius taikydamos šiuos kriterijus:

a. incidento priežastys priklauso kitos vietos institucijos reguliavimo kompetencijai (t. y. jos kompetencijos sričiai).
b. Incidento padariniai turi poveikį kitos vietos institucijos tikslams (pvz., išsaugoti finansinį stabilumą).
c. Incidentas turi arba gali turėti plataus masto poveikį mokėjimo paslaugų vartotojams.
d. Apie incidentą, tikėtina, visapusiškai praneš (arba jau pranešė) žiniasklaida.

5.2. Buveinės valstybės narės kompetentingos institucijos šį vertinimą incidento aktualumo laikotarpiu turėtų atlikti nuolat, siekdamos nustatyti galimus pokyčius, dėl kurių incidentas gali tapti aktualiu, jeigu anksčiau jis tokiu nebuvo laikomas.

6 gairė. Informacija, kuria turi būti dalijamasi

6.1. Neatsižvelgdamos į bet kurį kitą teisinį reikalavimą keistis su incidentu susijusia informacija su kitomis vietos institucijomis, kompetentingos institucijos informaciją apie didelius operacinius ar saugumo incidentus turėtų teikti atitinkamoms vietos institucijoms, nurodytoms taikant 5.1 gairę, bent jau tuo metu, kai gaunamas pradinis pranešimas (arba pranešimas, kuris paskatino keistis informacija) ir kai joms pranešama, kad sugrįžtama prie įprastos verslo eigos (t. y. kai gaunamas tarpinis pranešimas).

6.2. Kompetentingos institucijos turėtų atitinkamoms vietos institucijoms pateikti informaciją, reikalingą norint susidaryti aiškų vaizdą, kas įvyko ir kokie galimi padariniai. Siekdamos tai

padaryti, jos turėtų pateikti bent jau toliau nurodytuose šablono laukeliuose (pradiniame arba tarpiniame pranešime) mokėjimo paslaugų teikėjo nurodytą informaciją:

- incidento pripažinimo dideliu datą ir laiką;
- incidento aptikimo datą ir laiką;
- incidento pradžios datą ir laiką;
- incidento panaikinimo arba tikėtino panaikinimo datą ir laiką;
- trumpą incidento aprašymą (įskaitant nekonfidencialias išsamaus aprašymo dalis);
- trumpą priemonių, kurių imtasi arba planuojama imtis incidentui neutralizuoti, aprašymą;
- aprašymą, kokį poveikį incidentas galėtų turėti kitiems mokėjimo paslaugų teikėjams ir (arba) infrastruktūros objektams;
- pranešimų žiniasklaidoje (jeigu jų yra) aprašymą;
- incidento priežastį.

6.3. Prieš keisdamosi su atitinkamomis vietos institucijomis su incidentu susijusia informacija, prireikus, kompetentingos institucijos turėtų tinkamai užtikrinti informacijos anonimiškumą ir neperduoti jokios informacijos, kuriai galėtų būti taikomas konfidencialumas arba intelektinės nuosavybės apribojimai. Nepaisant to, kompetentingos institucijos turėtų atitinkamoms vietos institucijoms nurodyti pranešimą teikiančio mokėjimo paslaugų teikėjo pavadinimą ir adresą, jeigu minėtosios vietos institucijos gali užtikrinti, kad informacija bus tvarkoma konfidencialiai.

6.4. Kompetentingos institucijos turėtų visą laiką užtikrinti informacijos, kuri saugoma ir kuria keičiamasi su atitinkamomis vietos institucijomis, konfidencialumą ir vientisumą ir atitinkamoms vietos institucijoms tinkamai įrodyti savo tapatybę. Pirmiausia kompetentingos institucijos visai pagal šias gaires gautai informacijai turėtų taikyti MPD2 išdėstytus įpareigojimus saugoti profesinę paslaptį, nedarydamos poveikio taikytinai Sąjungos teisei ir nacionaliniams reikalavimams.

6. Kompetentingoms institucijoms skirtos gairės dėl kriterijų, kaip įvertinti aktualius pranešimų apie incidentus duomenis, kuriais bus keičiamasi su EBI ir ECB, ir dėl jų perdavimo formato ir procedūrų

7 gairė. Informacija, kuria turi būti dalijamasi

7.1. Kompetentingos institucijos turėtų EBI ir ECB visada pateikti visus iš didelio operacinio ar saugumo incidento paveiktų mokėjimo paslaugų teikėjų (arba jų vardu) gautus pranešimus naudodamos EBI svetainėje paskelbtą standartinę rinkmeną.

8 gairė. Komunikacija

8.1. Kompetentingos institucijos turėtų visą laiką užtikrinti informacijos, kuri saugoma ir kuria keičiamasi su EBI ir ECB, konfidencialumą ir vientisumą ir EBI bei ECB tinkamai įrodyti savo tapatybę. Pirmiausia kompetentingos institucijos visai pagal šias gaires gautai informacijai turėtų taikyti MPD2 išdėstytus įpareigojimus saugoti profesinę paslaptį, nedarydamos poveikio taikytinai Sąjungos teisei ir nacionaliniams reikalavimams.

8.2. Siekdamos išvengti vėlavimo perduoti su incidentu susijusią informaciją EBI ir (arba) ECB ir siekdamos padėti kuo labiau sumažinti veiklos sutrikdymo riziką, kompetentingos institucijos turėtų turėti galimybę naudotis tinkamomis komunikacijos priemonėmis.

1 priedas. Pranešimų teikimo šablonas mokėjimo paslaugų teikėjams

Pradinis pranešimas

Pradinis pranešimas	per 4 valandas po incidento pripažinimo dideliu		Atkurti
Pranešimo data (MMMM MM DD)		Laikas (*HH:MM*)	
Incidento kodas			

A. Pradinis pranešimas					
A 1. BENDRIEJI DUOMENYS					
Pranešimo tipas					
Pranešimo tipas					
Paveiktas mokėjimo paslaugų teikėjas (MPT)					
MPT pavadinimas					
MPT nacionalinis identifikavimo numeris					
Pagrindinis grupės subjektas, jeigu taikytina					
Incidento paveikta šalis / šalys	☐ AT ☐ BE ☐ BG ☐ CY ☐ CZ	☐ DE ☐ DK ☐ EE ☐ ES ☐ FI	☐ FR ☐ LI ☐ GR ☐ HR ☐ HU	☐ IE ☐ IS ☐ IT ☐ LT ☐ LU	☐ LV ☐ MT ☐ NL ☐ NO ☐ PL	☐ PT ☐ RO ☐ SE ☐ SI ☐ SK
Pagrindinis asmuo ryšiams		E. paštas		Telefonas		
Antrasis kontaktinis asmuo		E. paštas		Telefonas		
Pranešimą teikiantis subjektas (pildykite šį skirsnį, jeigu pranešimą teikiantis subjektas nėra paveiktas mokėjimo paslaugų teikėjas deleguotojo pranešimų teikimo atveju)					
Pranešimą teikiančio subjekto pavadinimas					
Nacionalinis identifikavimo Nr.					
Pagrindinis asmuo ryšiams		E. paštas		Telefonas		
Antrasis kontaktinis asmuo		E. paštas		Telefonas		
A 2. INCIDENTO APTIKIMAS IR KLASIFIKAVIMAS					
Incidento aptikimo data ir laikas (*MMMM MM DD HH:MM*)					
Incidento klasifikavimo data ir laikas (*MMMM MM DD HH:MM*)					
Incidentą aptiko		Jeigu „Kita“, paaiškinkite:			
Incidento tipas					
Kriterijai, dėl kurių parengiamas pranešimas apie didelį incidentą	☐ Paveiktos operacijos ☐ Paveikti mokėjimo paslaugų vartotojai ☐ Paslaugos nevykdymo ☐ Tinklų ir informacinių sistemų saugumo ☐ Ekonominis poveikis ☐ Aukšto lygio vidinė sklaida ☐ Kiti galbūt paveikti mokėjimo paslaugų teikėjai arba aktualūs infrastruktūros objektai ☐ Poveikis reputacijai				
Trumpas bendras incidento aprašymas					
Poveikis kitose ES valstybėse narėse, jei taikytina					
Pranešimas kitoms institucijoms		Jeigu taip, atsakykite išsamiau:			
Vėlavimo pateikti pradinį pranešimą priežastys					

Tarpinis pranešimas

Pranešimas apie didelį incidentą			
Tarpinis pranešimas	maks. per 3 darbo dienas nuo pradinio pranešimo pateikimo		Atkurti
Pranešimo data *(MMMM MM DD)*		Laikas *(HH:MM)*	
Incidento kodas			

B. Tarpinis pranešimas			
B 1. BENDRIEJI DUOMENYS			
Išsamesnis incidento aprašymas:			
Kokia yra konkreti problema?			
Kaip prasidėjo incidentas?			
Kokia buvo jo raida?			
Kokios yra pasekmės (visų pirma, mokėjimo paslaugų vartotojams)?			
Ar apie incidentą pranešta mokėjimo paslaugų vartotojams?		Jeigu taip, atsakykite išsamiau:	
Ar jis susijęs su ankstesniu (-iais) incidentu (-ais)?		Jeigu taip, atsakykite išsamiau:	
Ar buvo paveikti arba ar dalyvavo kiti paslaugų teikėjai / trečiosios šalys?		Jeigu taip, atsakykite išsamiau:	
Ar pradėtas krizės valdymas (vidaus ir (arba) išorės)?		Jeigu taip, atsakykite išsamiau:	
Incidento pradžios data ir laikas (jeigu jau nustatyta) *(MMMM MM DD HH:MM)*			
Incidento panaikinimo arba tikėtino panaikinimo data ir laikas *(MMMM MM DD HH:MM)*			
Paveiktos funkcinės srities	☐ Autentiškumo patvirtinimas/ ☐ Tiesioginis atsiskaitymas ☐ Ryšiai ☐ Netiesioginis ☐ Tarpuskaita ☐ Kita	Jeigu „Kita", paaiškinkite:	
Ankstesnių pranešimų pakeitimai			
B 2. INCIDENTO KLASIFIKAVIMAS IR INFORMACIJA APIE INCIDENTĄ			
Paveiktos operacijos [2]	Poveikio lygio Paveiktų operacijų skaičius Įprasto operacijų skaičiaus proc. dalis Paveiktų operacijų vertė EUR Incidento trukmė (taikoma tik operaciniams incidentams) Pastabos:		
Paveikti mokėjimo paslaugų vartotojai [3]	Poveikio lygio Paveiktų mokėjimo paslaugų vartotojų skaičius Bendro mokėjimo paslaugų vartotojų skaičiaus proc. dalis		
Tinklų ir informacinių sistemų saugumo pažeidimas	Aprašykite, kaip paveiktas tinklas ar informacinės sistemos		
Paslaugos nevykdymo laikas	Bendras paslaugos nevykdymo laikas:	Dienų: Valandų: Minučių:	
Ekonominis poveikis	Poveikio lygio Tiesioginės išlaidos EUR Netiesioginės išlaidos EUR		
Aukšto lygio vidinė sklaida	Aprašykite incidento vidinės sklaidos lygį, nurodydami, ar jis sukėlė arba, tikėtina, sukels krizinį (arba lygiavertį) režimą, ir jeigu taip, tai aprašykite		
Kiti galbūt paveikti mokėjimo paslaugų teikėjai arba aktualūs infrastruktūros objektai	Aprašykite, kokį poveikį incidentas galėtų turėti kitiems mokėjimo paslaugų teikėjams ir (arba) infrastruktūros objektams		
Poveikis reputacijai	Aprašykite, kokį poveikį incidentas galėtų turėti mokėjimo paslaugų teikėjo reputacijai (pvz., pranešimai žiniasklaidoje, ieškiniai ar teisės aktų pažeidimai...)		
B 3. INCIDENTO APRAŠYMAS			
Incidento tipas			
Incidento priežastis	☐ Vyksta tyrimas ☐ Kenkėjiškas veiksmas ☐ Proceso klaida ☐ Sistemos klaida ☐ Žmogaus klaida ☐ Išoriniai įvykiai ☐ Kita	Jeigu „Kita", paaiškinkite:	
Ar incidentas paveikė jus tiesiogiai, ar netiesiogiai per paslaugos teikėją?		Jeigu netiesiogiai, nurodykite paslaugos teikėjo pavadinimą	
B 4. INCIDENTO POVEIKIS			
Bendras poveikis	☐ Sąžiningumas ☐ Konfidencialumas ☐ Prieinamumas ☐ Autentiškumas		
Paveikti komerciniai kanalai	☐ Filialai ☐ Telefoninė bankininkystė ☐ Aptarnavimo punktas ☐ Elektroninė bankininkystė ☐ Mobiliojі bankininkystė ☐ Kita ☐ Elektroninė prekyba ☐ Bankomatai		
	Jeigu „Kita", paaiškinkite:		
Paveiktos mokėjimo paslaugos	☐ Grynųjų pinigų įnešimas į mokėjimo sąskaitą ☐ Kredito pervedimai ☐ Pinigų perlaida ☐ Pinigų išgryninimas iš mokėjimo sąskaitos ☐ Tiesioginis debetas ☐ Mokėjimo ☐ Operacijos, reikalingos mokėjimo sąskaitai tvarkyti ☐ Mokėjimai kortelėmis ☐ Informacijos apie sąskaitą paslaugos ☐ Mokėjimo priemonių įsigijimas ☐ Mokėjimo priemonių išdavimas		
B 5. INCIDENTO POVEIKIO SUMAŽINIMAS			
Kokių veiksmų ar priemonių iki šiol imtasi arba planuojama imtis incidento poveikiui neutralizuoti?			
Ar buvo aktyvuotas verslo tęstinumo planas ir (arba) nelaimių neutralizavimo planas?			
Jeigu taip, kada? *(MMMM MM DD HH:MM)*			
Jeigu taip, aprašykite			

Galutinis pranešimas

Pranešimas apie didelį incidentą

Pasirinkite pranešimo tipą:

per 20 darbo dienas nuo pradinio pranešimo pateikimo

Aprašykite:
(taikoma incidentams, kurie buvo perklasifikuoti kaip nedideli)

Atkurti išskleidžiamąją atranką

Pranešimo data (MMMM MM DD)
Incidento kodas

Laikas *(HH:MM)*

C. Galutinis pranešimas

Jeigu tarpinis pranešimas nebuvo siunčiamas, užpildykite ir B skirsnį

C 1. BENDRIEJI DUOMENYS

Pradinio pranešimo ir tarpinio (-ių) pranešimo (-ų) informacijos atnaujinimas	
Ankstesnių pranešimų pakeitimai	
Visa kitą svarbi informacija	
Ar taikomos visos pirminės kontrolės priemonės?	
Jeigu ne, nurodykite, kurios kontrolės priemonės nėra atkurtos ir kiek dar laiko reikia joms atkurti	

C 2. PAGRINDINĖS PRIEŽASTIES ANALIZĖ IR TOLESNI VEIKSMAI

Kokia buvo pagrindinė priežastis (jeigu ji jau žinoma)?

☐ Kenkėjiškas veiksmas ☐ Proceso klaida ☐ Sistemos klaida ☐ Žmogaus klaida ☐ Išorinis įvykis ☐ Kita

Nurodykite:

Kenkėjiškas veiksmas	Proceso klaida	Sistemos klaida	Žmogaus klaida	Išorinis įvykis
Kenkėjiškas kodas	Netinkama stebėsena ir kontrolė	Aparatinės	Netyčia	Tiekėjo / techninių paslaugų teikėjo neveikimas
Informacijos rinkimas	Ryšio problemos	Tinklo triktis	Neveikimas	*Force majeure*
Įsibrovimai	Netinkamas veikimas	Duomenų bazės	Nepakankami ištekliai	Kita
Paskirstytojo paslaugos trikdymo ataka (DDoS)	Netinkamas pokyčių valdymas	Programinės įrangos / taikomosios programos	Kita	
Tyčiniai vidaus veiksmai	Netinkamos vidaus procedūros ir dokumentacija	Fizinė žala		
Tyčinė išorinė fizinė žala	Atkūrimo problemos	Kita		
Informacijos turinio saugumas	Kita			
Sukčiavimas				
Kita				

Jeigu „Kita", paaiškinkite:

Kita svarbi informacija apie pagrindinę priežastį	
Pagrindiniai taisomieji veiksmai ir (arba) priemonės (jeigu jie jau žinomi), kurių imtasi arba planuojama imtis, kad incidentas nepasikartotų ateityje	

C 3. PAPILDOMA INFORMACIJA

Ar incidentas aptartas su kitais mokėjimo paslaugų teikėjais informavimo tikslais?	Jeigu taip, pateikite informaciją:
Ar prieš mokėjimo paslaugų teikėją imtasi kokių nors teisinių veiksmų?	Jeigu taip, pateikite informaciją:
Veiksmų, kurių imtasi, veiksmingumo vertinimas	Pateikite informaciją:

ŠABLONO PILDYMO INSTRUKCIJOS

Mokėjimo paslaugų teikėjai (MPT) turėtų užpildyti aktualų šablono skirsnį, priklausomai nuo esamo pranešimo etapo: A skirsnį, kai pildomas pradinis pranešimas, B skirsnį, kai pildomi tarpiniai pranešimai, ir C skirsnį, kai pildomas galutinis pranešimas. MPT turėtų naudoti tą patį šabloną pradiniam, tarpiniam ir galutiniam su tuo pačiu incidentu susijusiam pranešimui pateikti. Visi laukeliai yra privalomi, jeigu aiškiai nenurodyta kitaip.

Antraštė

Pradinis pranešimas: tai yra pirmas pranešimas, kurį mokėjimo paslaugų teikėjas teikia buveinės valstybės narės kompetentingai institucijai.

Tarpinis pranešimas: pateikiamas išsamesnis incidento ir jo padarinių aprašymas. Tai pradinio pranešimo dėl to paties incidento (ir kai taikytina, ankstesnio tarpinio pranešimo) atnaujinta versija.

Galutinis pranešimas: tai galutinis pranešimas, kurį mokėjimo paslaugų teikėjas siųs apie incidentą, nes i) jau atlikta pagrindinės priežasties analizė ir įverčius galima pakeisti faktiniais duomenimis arba ii) incidentas nebelaikomas dideliu ir jį reikia perklasifikuoti.

Incidentas perklasifikuotas kaip nedidelis: incidentas nebeatitinka didelio incidento kriterijų ir tikimasi, kad iki jo panaikinimo jis tų kriterijų nebeatitiks. MPT turėtų paaiškinti šio perklasifikavimo motyvus.

Pranešimo data ir laikas: tiksli pranešimo pateikimo kompetentingai institucijai data ir laikas.

Incidento kodas (taikomas tarpiniams ir galutiniams pranešimams, taip pat atnaujintoms pradinio pranešimo versijoms): kompetentingos institucijos suteiktas kodas, kai pateikiamas pradinis pranešimas, kad būtų galima nedviprasmiškai identifikuoti incidentą. Kiekviena kompetentinga institucija turėtų priekyje nurodyti savo atitinkamos valstybės narės 2 skaitmenų ISO kodą[2].

A - Pradinis pranešimas

A 1 - Bendrieji duomenys

Pranešimo tipas:

Individualus: pranešimas susijęs su vienu mokėjimo paslaugų teikėju.

Konsoliduotas: pranešimas susijęs su keliais MPT toje pačioje valstybėje narėje, kuriems padarė poveikį tas pats didelis operacinis ar saugumo incidentas ir kurie nusprendžia pateikti konsoliduotąjį pranešimą. Laukeliai *Paveiktas mokėjimo paslaugų teikėjas* turėtų būti palikti tušti (išskyrus laukelį *Incidento paveikta šalis / šalys*), o į pranešimą įtrauktų mokėjimo paslaugų teikėjų sąrašas turėtų būti pateiktas užpildant atitinkamą lentelę (*Konsoliduotasis pranešimas. Mokėjimo paslaugų teikėjų sąrašas*).

Paveiktas MPT: nurodomas incidentą patiriantis mokėjimo paslaugų teikėjas.

MPT pavadinimas: visas mokėjimo paslaugų teikėjo, kuriam taikoma pranešimų teikimo procedūra, pavadinimas, nurodytas taikytiname oficialiame nacionaliniame mokėjimo paslaugų teikėjų registre.

MPT nacionalinis identifikavimo Nr.: unikalus nacionalinis identifikavimo numeris, kurį buveinės valstybės narės kompetentinga institucija naudoja nacionaliniame registre MPT nedviprasmiškai identifikuoti.

Pagrindinis grupės subjektas: subjektų grupių, kaip apibrėžta MPD2 4 straipsnio 40 punkte, nurodykite pagrindinio subjekto pavadinimą.

Incidento paveikta šalis / šalys: šalis arba šalys, kuriose pasireiškė incidento poveikis (pvz., poveikį patyrė keli MPT filialai skirtingose šalyse), neatsižvelgiant į incidento sunkumą kitoje šalyje / kitose šalyse. Ta šalis nebūtinai turi sutapti su buveinės valstybe nare.

[2] Žr. alfa-2 šalių kodus pagal ISO-3166 adresu https://www.iso.org/iso-3166-country-codes.html.

Pagrindinis kontaktinis asmuo: paveikto mokėjimo paslaugų teikėjo darbuotojo – asmens, atsakingo už pranešimą apie incidentą, vardas ir pavardė arba, jeigu paveikto MPT vardu pranešimus teikia trečiasis paslaugų teikėjas – asmens, atsakingo už incidentų valdymo ir (arba) rizikos departamentą ar panašią sritį, vardas ir pavardė.

E. paštas: e. pašto adresas, kuriuo prireikus būtų galima siųsti prašymus pateikti papildomus paaiškinimus. Tai gali būti asmeninis arba įmonės e. pašto adresas.

Kontaktinis telefono numeris: telefono numeris, kuriuo prireikus galėtų būti siunčiami prašymai pateikti išsamesnį paaiškinimą. Tai gali būti asmeninis arba įstaigos telefono numeris.

Antrasis kontaktinis asmuo: alternatyvaus asmens, su kuriuo susisiekusi kompetentinga institucija gali pasiteirauti apie incidentą, jeigu pagrindinis kontaktinis asmuo yra nepasiekiamas, vardas ir pavardė. Jeigu paveikto MPT vardu pranešimus teikia trečiasis paslaugų teikėjas – paveikto mokėjimo paslaugų teikėjo incidentų valdymo ir (arba) rizikos departamento arba panašios srities darbuotojo vardas ir pavardė.

E. paštas: alternatyvaus kontaktinio asmens e. pašto adresas, kuriuo prireikus būtų galima siųsti prašymus pateikti papildomus paaiškinimus. Tai gali būti asmeninis arba įmonės e. pašto adresas.

Telefonas: alternatyvaus kontaktinio asmens telefono numeris, kuriuo prireikus būtų galima paprašyti pateikti papildomus paaiškinimus. Tai gali būti asmeninis arba įstaigos telefono numeris.

Pranešimą teikiantis subjektas: šis skirsnis turėtų būti pildomas, jeigu paveikto MPT vardu pranešimų teikimo įpareigojimus vykdo trečioji šalis, jei taikytina.

Pranešimą teikiančio subjekto pavadinimas: visas pranešimą apie incidentą teikiančio subjekto pavadinimas, nurodytas taikytiname oficialiame nacionaliniame verslo subjektų registre.

Nacionalinis identifikavimo numeris: unikalus nacionalinis identifikavimo numeris, naudojamas šalyje, kurioje yra trečioji šalis, apie incidentą pranešančiam subjektui nedviprasmiškai identifikuoti. Jeigu pranešimą teikianti trečioji šalis yra MPT, nacionalinis identifikavimo numeris turėtų būti unikalus nacionalinis MPT identifikavimo numeris, kurį nacionaliniame registre naudoja buveinės valstybės narės kompetentinga institucija.

Pagrindinis kontaktinis asmuo: už pranešimą apie incidentą atsakingo asmens vardas ir pavardė.

E. paštas: e. pašto adresas, kuriuo prireikus būtų galima siųsti prašymus pateikti papildomus paaiškinimus. Tai gali būti asmeninis arba įmonės e. pašto adresas.

Kontaktinis telefono numeris: telefono numeris, kuriuo prireikus turėtų būti siunčiami prašymai pateikti išsamesnį paaiškinimą. Tai gali būti asmeninis arba įstaigos telefono numeris.

Antrasis kontaktinis asmuo: pranešimą apie incidentą teikiančio subjekto alternatyvaus darbuotojo, su kuriuo kompetentinga institucija galėtų susisiekti, jeigu pagrindinis kontaktinis asmuo būtų nepasiekiamas, vardas ir pavardė.

E. paštas: alternatyvaus kontaktinio asmens e. pašto adresas, kuriuo prireikus būtų galima siųsti prašymus pateikti papildomus paaiškinimus. Tai gali būti asmeninis arba įmonės e. pašto adresas.

Telefonas: alternatyvaus kontaktinio asmens telefono numeris, kuriuo prireikus būtų galima paprašyti pateikti papildomus paaiškinimus. Tai gali būti asmeninis arba įstaigos telefono numeris.

A 2 - Incidento aptikimas ir klasifikavimas

Incidento aptikimo data ir laikas: data ir laikas, kai incidentas pirmą kartą buvo aptiktas.

Incidento klasifikavimo data ir laikas: data ir laikas, kai saugumo ar operacinis incidentas buvo pripažintas dideliu.

Incidentą aptiko: nurodykite, ar incidentą aptiko mokėjimo paslaugų vartotojas, MPT vidinė šalis (pvz., vidaus auditorius) arba kita išorinė šalis (pvz., paslaugų teikėjas). Jeigu tai nebuvo nė vienas iš nurodytų subjektų, atitinkamame laukelyje pateikite paaiškinimą.

Incidento tipas: nurodykite, ar, jūsų turimomis žiniomis ir jeigu yra informacijos, tai yra operacinis ar saugumo incidentas.

Operacinis: incidentas, kilęs dėl netinkamų ar savo funkcijos neatlikusių procesų, žmonių ir sistemų ar *force majeure* įvykių, turinčių neigiamą poveikį su mokėjimu susijusių paslaugų vientisumui, prieinamumui, konfidencialumui ir (arba) autentiškumui.

Saugumo: prieiga prie mokėjimo paslaugų teikėjo turto, jo naudojimas, atskleidimas, sutrikdymas, modifikavimas ar sunaikinimas, turintis neigiamą poveikį su mokėjimu susijusių paslaugų vientisumui, prieinamumui, konfidencialumui ir (arba) autentiškumui. Taip gali nutikti, be kita ko, kai MPT patiria tinklų ar informacinių sistemų saugumo pažeidimą.

Kriterijai, dėl kurių parengiamas pranešimas apie didelį incidentą: nurodykite, dėl kurių kriterijų parengtas pranešimas apie didelį incidentą. Galima pasirinkti kriterijų variantus: paveikti sandoriai, paveikti mokėjimo paslaugų vartotojai, paslaugos nevykdymo laikas, tinklų ar informacinių sistemų saugumo pažeidimas, ekonominis poveikis, aukšto lygio vidinė sklaida, kiti galbūt paveikti mokėjimo paslaugų teikėjai arba aktualūs infrastruktūros objektai ir (arba) poveikis reputacijai.

Trumpas bendras incidento aprašymas: trumpai paaiškinkite aktualiausius incidento aspektus, nurodydami galimas priežastis, nedelsiant pasireiškusį poveikį ir kt.

Poveikis kitose ES valstybėse narėse, jei taikytina: trumpai paaiškinkite poveikį, kurį incidentas padarė kitoje ES valstybėje narėje (pvz., mokėjimo paslaugų vartotojams, MPT ir (arba) mokėjimo infrastruktūros objektams). Jeigu įmanoma iki nustatyto pranešimo pateikimo termino, pateikite vertimą į anglų kalbą.

Pranešimo teikimas kitoms valdžios institucijoms: nurodykite, ar apie incidentą buvo / bus pranešta kitoms valdžios institucijoms atskirose pranešimo apie incidentus sistemose, jeigu tai žinoma pranešimo pateikimo metu. Jeigu taip, nurodykite atitinkamas valdžios institucijas.

Vėlavimo pateikti pradinį pranešimą priežastys: paaiškinkite priežastis, dėl kurių jums prireikė daugiau nei 24 valandų incidentui klasifikuoti.

B Tarpinis pranešimas

B 1 – Bendrieji duomenys

Išsamesnis incidento aprašymas: aprašykite pagrindinius incidento ypatumus pateikdami bent informaciją apie konkrečią problemą ir su ja susijusias aplinkybes, aprašymą, kaip incidentas prasidėjo ir kaip vyko jo raida, padarinius, ypač mokėjimo paslaugų vartotojams, ir kt. Taip pat pateikite informaciją apie bendravimą su mokėjimo paslaugų vartotojais, jei taikytina.

Ar jis susijęs su ankstesniu (-iais) incidentu (-ais)?: nurodykite, ar incidentas susijęs su ankstesniais incidentais, jeigu tokios informacijos yra. Jeigu incidentas susijęs su ankstesniais incidentais, nurodykite, su kuriais.

Ar buvo paveikti arba ar dalyvavo kiti paslaugų teikėjai / trečiosios šalys?: nurodykite, ar incidentas padarė poveikį kitiems paslaugų teikėjams / trečiosioms šalims arba ar jie jame dalyvavo, jeigu tokios informacijos yra. Jeigu incidentas paveikė kitus paslaugų teikėjus / trečiąsias šalis arba jie jame dalyvavo, išvardykite juos ir pateikite daugiau informacijos.

Ar pradėtas krizės valdymas (vidaus ir (arba) išorės)?: nurodykite, ar pradėtas krizės valdymas (vidaus ir (arba) išorės). Jeigu krizės valdymas pradėtas, pateikite daugiau informacijos.

Incidento pradžios data ir laikas: data ir laikas, kai incidentas prasidėjo, jeigu žinoma.

Data ir laikas, kai paslauga po incidento atkuriama: nurodykite datą ir laiką, kai incidentas buvo suvaldytas arba jį tikimasi suvaldyti ir buvo arba, tikėtina, bus sugrįžta prie įprastos verslo eigos.

Paveiktos funkcinės sritys: nurodykite mokėjimo proceso etapą ar etapus, kuriems incidentas padarė poveikį, kaip antai autentiškumo patvirtinimą / autorizavimą, bendravimą, tarpuskaitą, tiesioginį atsiskaitymą, netiesioginį atsiskaitymą ir kt.

Autentiškumo patvirtinimas / autorizavimas: procedūros, leidžiančios mokėjimo paslaugų teikėjui patikrinti mokėjimo paslaugų vartotojo tapatybę arba konkrečios mokėjimo priemonės galiojimą, įskaitant vartotojo personalizuotų saugumo požymių naudojimą ir mokėjimo paslaugų vartotojo (arba to vartotojo vardu veikiančios trečiosios šalies) duotą sutikimą pervesti lėšas.

Bendravimas: informacijos srautas identifikavimo, autentiškumo patvirtinimo, pranešimo ir informavimo tikslais tarp sąskaitą aptarnaujančio MPT ir mokėjimo inicijavimo paslaugų teikėjų, informacijos apie sąskaitą teikėjų, mokėtojų, gavėjų ir kitų MPT.

Tarpuskaita: pervedimo nurodymų perdavimo, suderinimo ir, kai kuriais atvejais, patvirtinimo prieš atsiskaitymą procesas, galintis apimti nurodymų užskaitą ir galutinių pozicijų sudarymą atsiskaitymams.

Tiesioginis atsiskaitymas: operacijos arba apdorojimo užbaigimas siekiant įvykdyti dalyvių prievoles lėšų pervedimu, kai šį veiksmą atlieka pats paveiktas MPT.

Netiesioginis atsiskaitymas: operacijos arba apdorojimo užbaigimas siekiant įvykdyti dalyvių prievoles lėšų pervedimu, kai šį veiksmą paveikto mokėjimo paslaugų teikėjo vardu atlieka kitas MPT.

Kita: paveikta funkcinė sritis nėra nė vienas iš paminėtų variantų. Tuščiame teksto laukelyje turėtų būti pateikta papildoma informacija.

Ankstesnių pranešimų pakeitimai: nurodykite ankstesniuose pranešimuose, susijusiuose su tuo pačiu incidentu (pvz., pradiniame arba, kai taikytina, tarpiniame pranešime), pateiktos informacijos pakeitimus.

B 2 – Incidento klasifikavimas ir informacija apie incidentą

Paveiktos operacijos: MPT nurodo, kokias ribas incidentas pasiekė arba, tikėtina, pasieks (jeigu tokios ribos yra), ir nurodo atitinkamus duomenis: paveiktų operacijų skaičių, paveiktų operacijų procentinę dalį nuo mokėjimo operacijų, atliktų teikiant tas pačias mokėjimo paslaugas, kurias paveikė incidentas, skaičiaus, ir bendrą operacijų vertę. MPT turėtų nurodyti konkrečias šių kintamųjų vertes, kurios gali būti arba faktiniai duomenys, arba įverčiai. Paprastai MPT paveiktomis operacijomis turėtų laikyti visas šalies vidaus ar tarpvalstybines operacijas, kurioms incidentas turėjo arba tikriausiai turės tiesioginį arba netiesioginį poveikį, ir ypač tas operacijas, kurių nebuvo įmanoma inicijuoti arba apdoroti, taip pat tas, kurių buvo pakeistas mokėjimo paskirties turinys, ir tas, kurias buvo pavesta atlikti apgaule (nesvarbu, ar lėšos buvo susigrąžintos, ar ne). Be to, mokėjimo paslaugų teikėjai įprastu mokėjimo operacijų lygiu turėtų laikyti šalies vidaus ir tarpvalstybinių mokėjimo operacijų, atliekamų teikiant incidento paveiktas mokėjimo paslaugas, kasdienį metinį vidurkį, o apskaičiavimų atskaitos laikotarpiu laikyti praėjusius metus. Jeigu MPT šio skaičiaus nelaiko reprezentatyviu (pvz., dėl sezoniškumo), jie turėtų naudoti kitą, reprezentatyvesnį rodiklį ir laukelyje *Pastabos* kompetentingai institucijai nurodyti atitinkamą šio metodo loginį pagrindą. Jeigu incidentas padarė poveikį mokėjimo operacijoms ne eurais, apskaičiuodami ribines vertes ir pranešdami apie operacijų vertę paveikti MPT turėtų konvertuoti operacijų sumą ne eurais į eurus pagal ECB paskelbtą prieš pranešimo apie incidentą pateikimą buvusios dienos pagrindinį valiutos keitimo kursą.

Paveikti mokėjimo paslaugų vartotojai: mokėjimo paslaugų teikėjai turėtų nurodyti, kokias ribas incidentas pasiekė arba, tikėtina, pasieks (jeigu tokios ribos yra), ir nurodyti atitinkamus duomenis: bendrą paveiktų mokėjimo paslaugų vartotojų skaičių ir paveiktų mokėjimo paslaugų vartotojų procentinę dalį nuo bendro mokėjimo paslaugų vartotojų skaičiaus. Mokėjimo paslaugų teikėjai turėtų nurodyti konkrečias šių kintamųjų vertes, kurios gali būti arba faktiniai duomenys, arba įverčiai. Paveiktais mokėjimo paslaugų vartotojais mokėjimo paslaugų teikėjai turėtų laikyti visus klientus (tiek šalies vidaus klientus, tiek klientus iš užsienio, tiek vartotojus, tiek įmones), turinčius sutartį su paveiktu MPT, pagal kurią jiems suteikiama teisė naudotis paveikta mokėjimo paslauga, ir patyrusius arba tikriausiai patirsiančius incidento padarinių. Remdamiesi ankstesne veikla, MPT turėtų apskaičiuoti įverčius, kad galėtų nustatyti, kiek mokėjimo paslaugų vartotojų galėjo naudotis mokėjimo paslauga incidento aktualumo laikotarpiu. Grupių atveju kiekvienas MPT turėtų atsižvelgti tik į savo mokėjimo paslaugų vartotojus. Kai MPT teikia veiklos paslaugas kitiems, tas MPT turėtų atsižvelgti tik į savo mokėjimo paslaugų vartotojus (jeigu jų yra), o tas veiklos paslaugas gaunantys MPT turėtų taip pat įvertinti incidentą atsižvelgdami į savo pačių mokėjimo paslaugų vartotojus. Be to, MPT bendru

mokėjimo paslaugų vartotojų skaičiumi turėtų laikyti bendrą šalies vidaus ir tarpvalstybinių mokėjimo paslaugų vartotojų, kurie incidento metu (arba pagal naujausius turimus duomenis) su jais turi sutartis ir turi teisę naudotis paveikta mokėjimo paslauga, skaičių, neatsižvelgdami į vartotojų dydį ir į tai, ar jie laikomi aktyviais, ar pasyviais mokėjimo paslaugų vartotojais.

Tinklų ir informacinių sistemų saugumo pažeidimas: MPT turėtų nustatyti, ar dėl kokių nors kenkėjiškų veiksmų sumažėjo su mokėjimo paslaugų teikimu susijusio tinklo ar informacinių sistemų (įskaitant duomenis) prieinamumas, autentiškumas, vientisumas arba konfidencialumas.

Paslaugos nevykdymo laikas: mokėjimo paslaugų teikėjai turėtų nurodyti, ar incidentas pasiekė arba, tikėtina, pasieks ribą, ir nurodyti atitinkamą skaičių – bendrą paslaugos nevykdymo laiką. MPT turėtų nurodyti konkrečias šio kintamojo vertes, kurios gali būti arba faktiniai duomenys, arba įverčiai. Mokėjimo paslaugų teikėjai turėtų apsvarstyti laikotarpį, kurį neveikia arba, tikėtina, neveiks bet kuri su mokėjimo paslaugų teikimu susijusi funkcija, procesas arba kanalas ir dėl to neįmanoma arba nebus įmanoma i) inicijuoti ir (arba) įvykdyti mokėjimo paslaugos ir (arba) ii) prisijungti prie mokėjimo sąskaitos. Paslaugos nevykdymo laiką MPT turėtų skaičiuoti nuo neveikimo pradžios ir, kai tai aktualu ir taikytina, turėtų atsižvelgti į savo darbo laiko intervalus, reikalingus mokėjimo paslaugoms įvykdyti, ir į nedarbo laiką bei techninės priežiūros laikotarpius. Jeigu mokėjimo paslaugų teikėjai negali nustatyti, kada nustojo būti vykdoma paslauga, paslaugos nevykdymo laiką išimties tvarka jie turėtų pradėti skaičiuoti nuo neveikimo aptikimo momento.

Ekonominis poveikis: MPT turėtų nurodyti, ar incidentas pasiekė arba, tikėtina, pasieks ribą, ir nurodyti atitinkamus duomenis – tiesiogines ir netiesiogines išlaidas. MPT turėtų nurodyti konkrečias šių kintamųjų vertes, kurios gali būti arba faktiniai duomenys, arba įverčiai. Mokėjimo paslaugų teikėjai turėtų atsižvelgti į išlaidas, kurias galima tiesiogiai susieti su incidentu, ir į išlaidas, kurios su incidentu susijusios netiesiogiai. Be kita ko, MPT turėtų atsižvelgti į nusavintas lėšas ar turtą, aparatinės ar programinės įrangos pakeitimo išlaidas, kitas teismo ar žalos atitaisymo išlaidas, mokesčius, mokėtinus dėl sutartinių prievolių nesilaikymo, sankcijas, išorės įsipareigojimus ir prarastas pajamas. Kalbant apie netiesiogines išlaidas, MPT turėtų atsižvelgti tik į tas išlaidas, kurios jau yra žinomos arba labai tikėtina, kad jos atsiras. Jeigu išlaidos yra ne eurais, apskaičiuodami ribines vertes ir pranešdami apie ekonominio poveikio vertę MPT turėtų konvertuoti išlaidų sumą ne eurais į eurus pagal ECB paskelbtą prieš pranešimo apie incidentą pateikimą buvusios dienos pagrindinį valiutos keitimo kursą.

> **Tiesioginės išlaidos:** incidento tiesiogiai sukeltos išlaidos (eurais), įskaitant išlaidas, reikalingas incidento padariniams pašalinti (pvz., nusavintoms lėšoms arba turtui grąžinti, aparatinei ir programinei įrangai pakeisti, sutartinių įsipareigojimų nesilaikymo mokesčiams sumokėti).
>
> **Netiesioginės išlaidos:** išlaidos (eurais), netiesiogiai sukeltos incidento (pvz., kliento teisių gynimo / kompensacijų išlaidos, galimos teisinės išlaidos).

Aukšto lygio vidinė sklaida: MPT turėtų apsvarstyti, ar dėl poveikio su mokėjimu susijusioms paslaugoms valdymo organas, kaip apibrėžta EBI IRT ir saugumo rizikos valdymo gairėse, pagal EBI IRT ir saugumo rizikos valdymo gairių 60 gairės d punktą buvo ar tikriausiai bus informuotas apie incidentą nesilaikant jokios periodinių pranešimų teikimo procedūros ir nuolat per visą incidento trukmę. Be to, mokėjimo paslaugų teikėjai turėtų apsvarstyti, ar dėl incidento poveikio su mokėjimu susijusioms paslaugoms yra arba bus pradėta dirbti krizės režimu.

Kiti galbūt paveikti MPT arba aktualūs infrastruktūros objektai: MPT turėtų įvertinti incidento poveikį finansų rinkai, kuri suprantama kaip finansų rinkos infrastruktūros objektai ir (arba) mokėjimo sistemos, kuriomis jie remiasi, taip pat likę MPT. Visų pirma MPT turėtų įvertinti, ar incidentas pasikartojo arba, tikėtina, pasikartos kitų MPT praktikoje, taip pat ar jis turėjo arba, tikėtina, turės poveikį sklandžiam finansų rinkos infrastruktūros objektų veikimui ir ar jis pakenkė arba, tikėtina, pakenks visos finansų sistemos patvarumui. Mokėjimo paslaugų teikėjai turėtų nepamiršti įvairių aspektų, pvz., ar paveiktas elementas ir (arba) programinė įranga yra nuosavybinė, ar visuotinai prieinama, ar sutrikdytas tinklas yra vidinis, ar išorinis, ir ar mokėjimo pasaugų teikėjas nutraukė arba, tikėtina, nutrauks savo prievolių vykdymą finansų rinkos infrastruktūros objektuose, kurių narys jis yra.

Poveikis reputacijai: MPT turėtų atsižvelgti į esamą arba, tikėtina, būsimą incidento matomumą rinkoje. Visų pirma MPT turėtų apsvarstyti tikimybę, kad incidentas padarys žalą visuomenei – patikimą rodiklį, kad incidentas gali turėti poveikį jų reputacijai. MPT turėtų atsižvelgti į tai, ar i) mokėjimo paslaugų vartotojai ir (arba) kiti MPT skundėsi dėl neigiamo incidento poveikio, ii) incidentas padarė poveikį matomam su mokėjimo paslauga susijusiam procesui ir todėl apie jį tikriausiai praneš arba jau pranešė žiniasklaida (ne tik tokia tradicinė žiniasklaida, kaip laikraščiai, bet ir tinklaraščiai, socialiniai tinklai ir kt.); tačiau pranešimas žiniasklaidoje šiuo atveju reiškia ne tik kelis sekėjų paskelbtus neigiamus komentarus, turėtų būti pagrįstas pranešimas arba didelis neigiamų komentarų / perspėjimų skaičius, iii) nebuvo ar tikriausiai nebus įvykdyti sutartiniai įsipareigojimai, tad mokėjimo paslaugų teikėjui bus pareikšta ieškinių, iv) nesilaikoma reguliuojamųjų reikalavimų ir dėl to taikomos priežiūros priemonės ar sankcijos, kurios buvo ar tikriausiai bus paskelbtos viešai, arba v) panašios rūšies incidentų jau buvę anksčiau.

B 3 – Incidento aprašymas

Incidento tipas: operacinis ar saugumo. papildomas paaiškinimas pateikiamas atitinkamame pradinio pranešimo laukelyje.

Incidento priežastis: nurodykite incidento priežastį arba, jeigu ji dar nežinoma – labiausiai tikėtiną priežastį. Galima pasirinkti iš kelių variantų.

Vyksta tyrimas: pažymėkite šį langelį, kai priežastis šiuo metu nežinoma.

Kenkėjiškas veiksmas: veiksmai, kuriais tyčia taikomasi į MPT. Tai, be kita ko, kenkėjiškas kodas, informacijos rinkimas, įsibrovimas, paskirstytojo paslaugos trikdymo ataka (D/DoS), tyčiniai vidaus veiksmai, tyčinė išorės fizinė žala, informacijos turinio saugumas, sukčiavimas ir kt. Išsamiau žr. šio šablono C2 skirsnį.

Proceso klaida: incidento priežastis buvo netinkamas mokėjimo proceso, proceso kontrolės priemonių ir (arba) pagalbinių procesų (pvz., pakeitimo ir (arba) perkėlimo, bandymo, konfigūravimo, pajėgumo, stebėsenos) parengimas ar įvykdymas.

Sistemos klaida: incidento priežastis susijusi su netinkamu mokėjimo veiklą palaikančių sistemų, tinklų, infrastruktūros objektų ir duomenų bazių parengimu, vykdymu, elementais, specifikacijomis, integravimu ar sudėtingumu.

Žmogaus klaida: incidentą sukėlė netyčinė žmogaus klaida – tai gali būti mokėjimo procedūros dalis (pvz., į mokėjimų sistemą įkeliama netinkama mokėjimų komandų rinkmena) arba kaip nors su ja susijusi priežastis (pvz., atsitiktinai nutrūksta elektros energijos tiekimas ir mokėjimo veikla sustabdoma).

Išoriniai įvykiai: priežastis yra susijusi su įvykiais, kurių organizacija paprastai negali tiesiogiai kontroliuoti (pvz., gaivalinėmis nelaimėmis, techninių paslaugų teikėjo klaida).

Kita: incidento priežastis nėra nė vienas iš paminėtų variantų. Tuščiame teksto laukelyje turėtų būti pateikta papildoma informacija.

Ar incidentas paveikė jus tiesiogiai, ar netiesiogiai per paslaugos teikėją?: nurodykite, ar incidentas buvo nukreiptas tiesiogiai prieš MPT arba paveikė jį netiesiogiai per trečiąją šalį, jei tokios informacijos yra. Netiesioginio poveikio atveju nurodykite paslaugos teikėjo (-ų) pavadinimą.

B 4 – Incidento poveikis

Bendras poveikis: nurodykite, kuriems aspektams operacinis ar saugumo incidentas padarė poveikį. Galima pasirinkti iš kelių variantų.

Vientisumas: turto (įskaitant duomenis) tikslumo ir visumos išsaugojimo ypatybė.

Prieinamumas: tokia su mokėjimu susijusių paslaugų ypatybė, kad prie jų gali gauti visapusišką prieigą ir jomis naudotis mokėjimo paslaugų vartotojai, laikantis priimtinų iš anksto nustatytų lygių.

Konfidencialumas: tokia ypatybė, kad informacija nepadaroma prieinama ir neatskleidžiama leidimo neturintiems asmenims, subjektams ar procesams.

Autentiškumas: tokia ypatybė, kai šaltinis yra tai, kas teigia esąs.

Paveikti komerciniai kanalai: nurodykite incidento paveiktą sąveikos su mokėjimo paslaugų vartotojais kanalą ar kanalus. Galima pažymėti kelis langelius.

Filialai: verslo vieta (ne pagrindinė buveinė), kuri yra mokėjimo paslaugų teikėjo dalis, nėra atskiras juridinis asmuo ir tiesiogiai atlieka kai kurias arba visas mokėjimo paslaugų teikėjo verslui būdingas operacijas. Visos verslo vietos, kurias toje pačioje valstybėje narėje įsteigė mokėjimo paslaugų teikėjas, turintis pagrindinę buveinę kitoje valstybėje narėje, turėtų būti laikomos vienu filialu.

Elektroninė bankininkystė: kompiuterių naudojimas finansinėms operacijoms internetu atlikti.

Telefoninė bankininkystė: telefonų naudojimas finansinėms operacijoms atlikti.

Mobilioji bankininkystė: specialių taikomųjų bankininkystės programų naudojimas išmaniajame telefone arba panašiame įrenginyje finansinėms operacijoms atlikti.

Bankomatai: elektromechaniniai įrenginiai, sudarantys mokėjimo paslaugų vartotojams sąlygas iš savo sąskaitų išgryninti pinigus ir (arba) prisijungti prie kitų paslaugų.

Pardavimo vieta: fizinės pardavėjo patalpos, kuriose inicijuojama mokėjimo operacija.

E. prekyba: mokėjimo operacija inicijuojama virtualioje pardavimo vietoje (pvz., mokėjimus inicijuojant internetu naudojant kredito pervedimus, mokėjimo korteles, elektroninių pinigų pervedimus iš vienos e. pinigų sąskaitos į kitą).

Kita: paveiktas komercinis kanalas nėra nė vienas iš paminėtų variantų. Tuščiame teksto laukelyje turėtų būti pateikta papildoma informacija.

Paveiktos mokėjimo paslaugos: nurodykite mokėjimo paslaugas, kurios dėl incidento tinkamai nevykdomos. Galima pažymėti kelis langelius.

Grynųjų pinigų įnešimas į mokėjimo sąskaitą: grynųjų pinigų įteikimas mokėjimo paslaugų teikėjui siekiant perkelti juos į mokėjimo sąskaitą.

Pinigų išgryninimas iš mokėjimo sąskaitos: mokėjimo paslaugų teikėjo gautas mokėjimo paslaugų vartotojo prašymas išduoti grynuosius pinigus ir atitinkama suma sumažinti jo mokėjimo sąskaitą.

Operacijos, reikalingos mokėjimo sąskaitai aptarnauti: veiksmai, kuriuos reikia atlikti mokėjimo sąskaitoje siekiant ją aktyvuoti, deaktyvuoti ir (arba) išlaikyti (pvz., atidaryti, užblokuoti).

Mokėjimo priemonių įgijimas: mokėjimo paslauga, kurią sudaro mokėjimo paslaugų teikėjo susitarimas su gavėju priimti ir apdoroti mokėjimo operacijas, kuriomis lėšos pervedamos gavėjui.

Kredito pervedimas: mokėjimo paslauga, kai mokėjimo paslaugų teikėjas, turintis mokėtojo mokėjimo sąskaitą, mokėtojo nurodymu į gavėjo mokėjimo sąskaitą atlieka mokėjimo operaciją arba kelias mokėjimo operacijas iš mokėtojo mokėjimo sąskaitos.

Tiesioginis debetas: mokėjimo paslauga, kuria debetuojama mokėtojo mokėjimo sąskaita, kai gavėjas, turėdamas gavėjui, gavėjo mokėjimo paslaugų teikėjui arba paties mokėtojo mokėjimo paslaugų teikėjui mokėtojo duotą sutikimą, inicijuoja mokėjimo operaciją.

Mokėjimai kortele: mokėjimo paslauga, pagrįsta mokėjimo kortelės sistemos infrastruktūra ir verslo taisyklėmis mokėjimo operacijai atlikti, kai naudojama kortelė, telekomunikacijos, skaitmeninis ar IT įrenginys arba programinė įranga, jeigu tokiu būdu atliekama debetinės ar kreditinės kortelės operacija. Kortele pagrįstos mokėjimo operacijos neapima kitokiomis mokėjimo paslaugomis pagrįstų operacijų.

Mokėjimo priemonių išleidimas: mokėjimo paslauga, kai mokėjimo paslaugų teikėjas susitaria su mokėtoju, kad mokėtojui bus išduota mokėjimo priemonė mokėtojo mokėjimo operacijoms inicijuoti ir apdoroti.

Pinigų perlaida: mokėjimo paslauga, kai mokėtojas perveda lėšas be jokios mokėtojo ar gavėjo vardu sukurtos sąskaitos, vien tik siekdamas pervesti atitinkamą sumą gavėjui ar gavėjo vardu veikiančiam kitam mokėjimo paslaugų teikėjui, o šios lėšos gaunamos gavėjo vardu ir jam perduodamos.

Mokėjimo inicijavimo paslaugos: mokėjimo paslaugos, kuriomis mokėjimo paslaugos vartotojo prašymu inicijuojamas mokėjimo nurodymas, susijęs su kito mokėjimo paslaugų teikėjo administruojama mokėjimo sąskaita.

Informavimo apie sąskaitas paslaugos: internetinės mokėjimo paslaugos, kuriomis teikiama konsoliduota informacija apie mokėjimo paslaugų vartotojo vieną ar daugiau mokėjimo sąskaitų, kurias administruoja kitas mokėjimo paslaugų teikėjas arba daugiau negu vienas mokėjimo paslaugų teikėjas.

B 5 – Incidento poveikio sumažinimas

Kokių veiksmų ar priemonių iki šiol imtasi arba planuojama imtis incidento poveikiui neutralizuoti?: pateikite išsamią informaciją apie veiksmus, kurių imtasi arba planuojama imtis siekiant laikinai išspręsti incidentą.

Ar buvo aktyvuoti verslo tęstinumo planai ir (arba) nelaimių neutralizavimo planai?: nurodykite, taip ar ne, ir jeigu taip, tai pateikite aktualiausią informaciją apie tai, kas įvyko (t. y. kada jie buvo aktyvuoti ir kas tuose planuose numatyta).

C – Galutinis pranešimas

C 1 – Bendrieji duomenys

Pradinio pranešimo ir tarpinio (-ių) pranešimo (-ų) informacijos atnaujinimas (santrauka): pateikite papildomos informacijos apie incidentą, įskaitant konkrečius tarpiniame pranešime pateiktos informacijos pokyčius. Taip pat pateikite visą kitą susijusią informaciją.

Ar taikomos visos pirminės kontrolės priemonės?: nurodykite, ar MPT turėjo panaikinti ar sumažinti kai kurias kontrolės priemonės kada nors incidento metu. Jeigu taip, nurodykite, ar visos kontrolės priemonės vėl taikomos, ir, jeigu ne, paaiškinkite laisva forma, kurios kontrolės priemonės nėra atkurtos ir kiek dar laiko reikia joms atkurti.

C 2 – Pagrindinės priežasties analizė ir tolesni veiksmai

Kokia buvo pagrindinė priežastis, jeigu ji jau žinoma?: nurodykite, kokia yra pagrindinė incidento priežastis arba, jeigu ji dar nežinoma, labiausiai tikėtiną priežastį. Galima pasirinkti iš kelių variantų. (Įsidėmėkite, kad pagrindinę priežastį reikėtų atskirti nuo incidento poveikio.)

Kenkėjiškas veiksmas: išorės ar vidaus veiksmai, kuriais tyčia taikomasi į MPT. Jie suskirstomi į šias kategorijas:

Kenkėjiškas kodas: pvz., virusas, kirminas, Trojos arklys, šnipinėjimo programa.

Informacijos rinkimas: pvz., skenavimas, ieškojimas, socialinė inžinerija.

Įsibrovimai: pvz., privilegijuotųjų sąskaitų pažeidimas, neprivilegijuotųjų sąskaitų pažeidimas, taikomųjų programų pažeidimas, botas.

Paskirstytojo paslaugos trikdymo ataka (DDoS) ataka: bandymas padaryti internetinę paslaugą neprieinamą perkraunant ją srautu iš daugelio šaltinių.

Tyčiniai vidaus veiksmai: pvz., sabotažas, vagystė.

Tyčinė išorės fizinė žala: pvz., sabotažas, fizinė patalpų / duomenų centrų ataka.

Informacijos turinio saugumas: neteisėta prieiga prie informacijos, neteisėtas informacijos pakeitimas.

Sukčiavimas: neteisėtas išteklių, autorių teisių, naudojimas, suklastotos tapatybės ataka, duomenų viliojimas.

Kita (nurodykite): incidento priežastis nėra nė vienas iš paminėtų variantų. Tuščiame teksto laukelyje turėtų būti pateikta papildoma informacija.

Proceso klaida: incidento priežastis buvo netinkamas mokėjimo proceso, proceso kontrolės priemonių ir (arba) pagalbinių procesų (pvz., pakeitimo ir (arba) perkėlimo, bandymo, konfigūravimo, pajėgumo, stebėsenos) parengimas ar įvykdymas. Jos suskirstomos į šias kategorijas:

Nepakankama stebėsena ir kontrolė: pvz., dėl einamųjų operacijų, sertifikatų galiojimo pabaigos datų, licencijų galiojimo pabaigos datų, pataisų galiojimo pabaigos datų, nustatytų maksimalių skaitiklių verčių, duomenų bazių užpildymo lygių, vartotojų teisių valdymo, dvejopos kontrolės principo.

Ryšio problemos: pvz., tarp rinkos dalyvių arba organizacijos viduje.

Netinkamas veikimas: pvz., nesikeičiama sertifikatais, sparčioji atmintis yra pilna.

Netinkamas pakeitimų valdymas: pvz., nenustatytos konfigūracijos klaidos, diegimas, įskaitant naujinius, techninės priežiūros problemos, netikėtos klaidos.

Vidaus procedūrų ir dokumentų nepakankamumas: pvz., nepakankamas skaidrumas, susijęs su funkcijomis ir procesais, triktys, dokumentų nebuvimas.

Atkūrimo problemos: pvz., nenumatytų atvejų valdymas, netinkamas atsarginių kopijų saugojimas.

Kita (nurodykite): incidento priežastis nėra nė vienas iš paminėtų variantų. Tuščiame teksto laukelyje turėtų būti pateikta papildoma informacija.

Sistemos klaida: incidento priežastis susijusi su netinkamu mokėjimo veiklą palaikančių sistemų, tinklų, infrastruktūros objektų ir duomenų bazių parengimu, vykdymu, elementais, specifikacijomis, integravimu ar sudėtingumu. Jos suskirstomos į šias kategorijas:

Aparatinės įrangos triktis: fizinės techninės įrangos, kurioje veikia procesai ir (arba) saugomi duomenys, kurių reikia MPT su mokėjimais susijusiai veiklai vykdyti, triktis (pvz., standžiųjų diskų, duomenų centrų, kitų infrastruktūros objektų triktis).

Tinklo triktis: viešų ar privačių telekomunikacijų tinklų, kuriuos gali būti keičiamasi duomenimis ir informacija (pvz., internetu) mokėjimo proceso metu, triktis.

Duomenų bazės problemos: duomenų struktūra, kurioje saugoma asmeninė ir su mokėjimu susijusi informacija, reikalinga mokėjimo operacijoms atlikti.

Programinės įrangos / taikomosios programos triktis: programų, operacinių sistemų ir kt., kuriose palaikomas MPT teikiamų mokėjimo paslaugų teikimas, triktis (pvz., gedimas, nežinomos funkcijos).

Fizinė žala: pvz., netyčinė žala, kurią sukelia netinkamos sąlygos, statybos darbai.

Kita (nurodykite): incidento priežastis nėra nė vienas iš paminėtų variantų. Tuščiame teksto laukelyje turėtų būti pateikta papildoma informacija.

Žmogaus klaida: incidentą sukėlė netyčinė žmogaus klaida – tai gali būti mokėjimo procedūros dalis (pvz., į mokėjimų sistemą įkeliama netinkama mokėjimų komandų rinkmena) arba kaip nors su ja susijusi priežastis (pvz., atsitiktinai nutrūksta elektros energijos tiekimas ir mokėjimo veikla sustabdoma). Jos suskirstomos į šias kategorijas:

Netyčinė: pvz., klaidos, praleidimai, nepakankama patirtis ir žinios.

Neveikimas: pvz., dėl įgūdžių, žinių, patirties, suvokimo trūkumo.

Nepakankami ištekliai: pvz., nepakankami žmogiškieji ištekliai, personalas.

Kita (nurodykite): incidento priežastis nėra nė vienas iš paminėtų variantų. Tuščiame teksto laukelyje turėtų būti pateikta papildoma informacija.

Išorinis įvykis: priežastis yra susijusi su įvykiais, kurių organizacija paprastai negali kontroliuoti. Jie suskirstomi į šias kategorijas:

Tiekėjo / techninių paslaugų teikėjo neveikimas: pvz., elektros atjungimas, interneto atjungimas, teisinės problemos, verslo problemos, paslaugų priklausomumas.

***Force majeure*:** pvz., elektros tiekimo sutrikimas, gaisrai, gamtinės priežastys, kaip antai žemės drebėjimai, potvyniai, gausūs krituliai, smarkus vėjas.

Kita (nurodykite): incidento priežastis nėra nė vienas iš paminėtų variantų. Tuščiame teksto laukelyje turėtų būti pateikta papildoma informacija.

Kita: incidento priežastis nėra nė vienas iš paminėtų variantų. Tuščiame teksto laukelyje turėtų būti pateikta papildoma informacija.

Kita svarbi informacija apie pagrindinę priežastį: nurodykite papildomą informaciją apie pagrindinę priežastį, įskaitant preliminarias išvadas, padarytas remiantis pagrindinės priežasties analize.

Pagrindiniai taisomieji veiksmai / priemonės, kurių imtasi arba planuojama imtis, kad incidentas nepasikartotų ateityje, jeigu jie jau žinomi: aprašykite pagrindinius veiksmus, kurių imtasi arba planuojama imtis, kad incidentas nepasikartotų ateityje.

C 3 – Papildoma informacija

Ar informacija apie incidentą pasidalyta su kitais MPT informacijos tikslais?: pateikite apžvalgą, su kuriais mokėjimo paslaugų teikėjais buvo oficialiai ar neoficialiai susisiekta turint tikslą jiems perduoti informaciją apie incidentą, pateikite mokėjimo paslaugų teikėjų, kurie buvo informuoti, duomenis, nurodykite informaciją, kuria buvo apsikeista, ir pagrindines pasidalijimo šia informacija priežastis.

Ar prieš mokėjimo paslaugų teikėją imtasi teisinių veiksmų?: nurodykite, ar galutinio pranešimo pildymo metu dėl incidento prieš mokėjimo paslaugų teikėją yra imtasi kokių nors teisinių veiksmų (pvz., ar jam yra pateiktas ieškinys, o gal jis prarado licenciją).

Veiksmų, kurių imtasi, veiksmingumo vertinimas: jeigu yra, pateikite veiksmų, kurių imtasi incidento metu, veiksmingumo įsivertinimą, įskaitant per incidentą įgytą patirtį.