EBA/GL/2017/10

19/12/2017

Gairės

dėl pranešimų apie didelius incidentus pagal Direktyvą (ES) 2015/2366 (MPD2)

1. Atitiktis gairėms ir informavimo pareiga

Šių gairių statusas

1. Šiame dokumente pateiktos pagal Reglamento (ES) Nr. 1093/2010 [1] 16 straipsnį parengtos gairės. Pagal Reglamento Nr. 1093/2010 16 straipsnio 3 dalį kompetentingos institucijos ir finansų įstaigos turi 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. Reglamento (ES) Nr. 1093/2010 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 pirmiausia yra skiriamos įstaigoms.

Pranešimo reikalavimai

3. Pagal Reglamento Nr. 1093/2010 16 straipsnio 3 dalį kompetentingos institucijos iki 19/02/2018. privalo EBI pranešti, ar laikosi arba ketina laikytis šių gairių, arba nurodyti nesilaikymo priežastis. Jeigu kompetentingos institucijos iki šio termino nepateiks jokio pranešimo, EBI laikys, kad jos gairių nesilaiko. Pranešimus reikėtų siųsti adresu compliance@eba.europa.eu užpildžius EBI interneto svetainėje pateiktą formą ir įrašius nuorodą „EBA/GL/2017/10“. Pranešimus turėtų teikti asmenys, turinys įgaliojimus pranešti apie gairių laikymąsi savo kompetentingų institucijų vardu. Apie visus gairių laikymosi pasikeitimus taip pat būtina pranešti EBI.

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 sąvokų 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 minėtosios direktyvos 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 minėtos direktyvos 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 Direktyvos (ES) 2015/2366 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 netyčiniai.

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 būdu sutrinka mokėjimo paslaugų teikėjo gebėjimas toliau vykdyti mokėjimo veiklą).

Adresatai

12. Pirmosios gairės (4 skirsnis) skiriamos mokėjimo paslaugų teikėjams, apibrėžtiems Direktyvos (ES) 2015/2366 4 straipsnio 11 punkte ir nurodytiems Reglamento (ES) 1093/2010 4 straipsnio 1 punkte.

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

Sąvokų apibrėžtys

14. Jei nenurodyta kitaip, Direktyvoje (ES) 2015/2366 vartojamos ir apibrėžtos sąvokos 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, autentiškumui ir (arba) tęstinumui.
Vientisumas	Turto (įskaitant duomenis) tikslumo ir visumos išsaugojimo ypatybė.
Prieinamumas	Tokia su mokėjimu susijusių paslaugų ypatybė, kad prie jų gali gauti prieigą ir jomis naudotis mokėjimo paslaugų vartotojai.
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.
Tęstinumas	Tokia ypatybė, kai organizacijos procesai, funkcijos ir turtas, reikalingi su mokėjimu susijusioms paslaugoms teikti, yra visapusiškai prieinami ir veikia iš anksto apibrėžtais prieinamais lygmenimis.
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 data

15. Šios gairės taikomos nuo 2018 m. sausio 13 d.

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

1 gairė. Priskyrimas dideliems incidentams

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 išdėstyta 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. Paslaugos neveikimo 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.

iv. 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).

v. Aukšto lygio vidinė sklaida

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

vi. Kiti galbūt paveikti mokėjimo paslaugų teikėjai arba susiję 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 kortelių sistemoms.

vii. 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).

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. 1 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.

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. Paslaugos neveikimo 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 neveikimo 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 neveikimo laiką išimties tvarka jie turėtų pradėti skaičiuoti nuo neveikimo aptikimo momento.

iv. 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.

v. *Aukšto lygio vidinė sklaida*

Mokėjimo paslaugų teikėjai turėtų apsvarstyti, ar dėl poveikio su mokėjimu susijusioms paslaugoms apie incidentą ne pagal periodinių pranešimų procedūrą ir nuolat per visą incidento aktualumo laikotarpį bus pranešama vyriausiajam informacijos pareigūnui (arba panašiam pareigūnui). Be to, mokėjimo paslaugų teikėjai turėtų apsvarstyti, ar dėl incidento poveikio su mokėjimu susijusioms paslaugoms yra arba bus pradėta dirbti krizės režimu.

vi. *Kiti galbūt paveikti mokėjimo paslaugų teikėjai arba susiję infrastruktūros objektai*

Mokėjimo paslaugų teikėjai turėtų įvertinti incidento poveikį finansų rinkai, kuri suprantama kaip finansų rinkos infrastruktūros objektai ir (arba) mokėjimo kortelių sistemos, kuriomis jie remiasi, taip pat kiti 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.

vii. *Poveikis reputacijai*

Mokėjimo paslaugų teikėjai turėtų atsižvelgti į esamą arba, tikėtina, būsimą incidento pastebimumą 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) incidentas sukėlė pastebimą procesą ir todėl tikėtina, kad apie jį praneš arba jau pranešė žiniasklaida (įvertinant ne tik tradicinę žiniasklaidą, pvz., laikraščius, bet ir tinklaraščius, socialinius tinklus ir kt.), ii) nebuvo arba tikriausiai nebus įvykdytos administracinės prievolės, iii) nebuvo arba tikriausiai nebus laikomasi sankcijų arba iv) tokio pat pobūdžio incidentas jau yra įvykęs anksčiau.

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

1 lentelė. Ribos

Kriterijai	Mažesnis poveikio lygis	Didesnis poveikio lygis
Paveiktos operacijos	> 10 % mokėjimo paslaugų teikėjo įprasto operacijų lygio (pagal operacijų skaičių) **ir** > 100 000 EUR	> 25 % mokėjimo paslaugų teikėjo įprasto operacijų lygio (pagal operacijų skaičių) **arba** > 5 mln. EUR
Paveikti mokėjimo paslaugų vartotojai	> 5 000 **ir** > 10 % mokėjimo paslaugų teikėjo mokėjimo paslaugų vartotojų	> 50 000 **arba** > 25 % mokėjimo paslaugų teikėjo mokėjimo paslaugų vartotojų
Paslaugos neveikimo laikas	> 2 valandos	Netaikoma
Ekonominis poveikis	Netaikoma	> Maks. (0,1 % 1 lygio kapitalo,* 200 000 EUR) **arba** > 5 mln. EUR
Aukšto lygio vidinė sklaida	Taip	Taip, ir tikriausiai bus pradėta dirbti kriziniu (arba lygiaverčiu) režimu
Kiti galbūt paveikti mokėjimo paslaugų teikėjai arba susiję infrastruktūros objektai	Taip	Netaikoma
Poveikis reputacijai	Taip	Netaikoma

*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 išsprendimo, 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.

2 gairė. Pranešimo procesas

2.1. Mokėjimo paslaugų teikėjai turėtų rinkti visą aktualią informaciją, naudodami 1 priede pateiktą šabloną parengti pranešimą apie incidentą ir jį pateikti buveinės valstybės narės kompetentingai institucijai. Mokėjimo paslaugų teikėjai turėtų užpildyti šabloną, vadovaudamiesi 1 priede pateiktais nurodymais.

2.2. Naudodamiesi tuo pačiu šablonu, mokėjimo paslaugų teikėjai turėtų informuoti kompetentingą instituciją visą incidento aktualumo laiką (pvz., pateikti pradinį, tarpinį ir galutinį pranešimus, kaip aprašyta 2.7–2.21 dalyse). Mokėjimo paslaugų teikėjai šabloną turėtų pildyti laipsniškai, nurodydami vis daugiau informacijos, kai tik jie ją sužino atlikdami savo vidinius tyrimus.

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. Jeigu esama papildomos informacijos ir kompetentinga institucija ją laiko aktualia, mokėjimo paslaugų teikėjai turėtų buveinės valstybės narės kompetentingai institucijai pateikti bet kokią papildomą informaciją, prie standartizuoto šablono kaip vieną ar keletą priedų pridėdami papildomą dokumentaciją.

2.5. Mokėjimo paslaugų teikėjai turėtų vykdyti bet kokius buveinės valstybės narės kompetentingos institucijos prašymus pateikti papildomą informaciją ar paaiškinimus dėl jau pateiktos dokumentacijos.

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.

Pirminis pranešimas

2.7. Mokėjimo paslaugų teikėjai turėtų buveinės valstybės narės kompetentingai institucijai pateikti pirminį pranešimą, kai nustatomas didelis operacinis ar saugumo incidentas.

2.8. Mokėjimo paslaugų teikėjai pirminį pranešimą kompetentingai institucijai turėtų nusiųsti per 4 valandas nuo didelio operacinio ar saugumo incidento aptikimo momento arba, jeigu

žinoma, kad tuo metu kompetentingos institucijos pranešimų priėmimo kanalai neprieinami arba neveikia – tada, kai jie vėl taps prieinami ir (arba) pradės veikti.

2.9. Mokėjimo paslaugų teikėjai turėtų buveinės valstybės narės kompetentingai institucijai taip pat pateikti pirminį pranešimą, kai anksčiau aptiktas nedidelis incidentas tampa dideliu incidentu. Šiuo konkrečiu atveju mokėjimo paslaugų teikėjai turėtų kompetentingai institucijai nusiųsti pirminį 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.

2.10. Mokėjimo paslaugų teikėjai į savo pirminius pranešimus (t. y. šablono A skirsnyje) turėtų įtraukti preliminarią informaciją, taip apibūdindami kai kurias pagrindines incidento savybes ir tikėtinus jo padarinius, grindžiamus informacija, kuri tapo prieinama iš karto po to, kai incidentas buvo aptiktas arba perklasifikuotas. Kai faktinių duomenų nėra, mokėjimo paslaugų teikėjai turėtų remtis apytikriais vertinimais. Mokėjimo paslaugų teikėjai į savo pirminį pranešimą taip pat turėtų įtraukti kito informacijos atnaujinimo datą, kuri turėtų būti kuo ankstesnė ir jokiomis aplinkybėmis ne vėlesnė kaip po 3 darbo dienų.

Tarpinis pranešimas

2.11. Mokėjimo paslaugų teikėjai turėtų teikti tarpinius pranešimus kiekvieną kartą, kai mano, kad esama aktualaus būklės pasikeitimo, ir bent jau iki ankstesniame pranešime (pirminiame pranešime arba ankstesniame tarpiniame pranešime) nurodytos kito atnaujinimo datos.

2.12. Mokėjimo paslaugų teikėjai kompetentingai institucijai turėtų pateikti pirmąjį tarpinį pranešimą su išsamesniu incidento ir jo padarinių aprašymu (šablono B skirsnis). Be to, mokėjimo paslaugų teikėjai turėtų parengti papildomus tarpinius pranešimus atnaujindami šablono A ir B skirsniuose jau pateiktą informaciją bent jau tada, kai jie sužino naują aktualią informaciją arba sužino apie didelius pokyčius nuo ankstesniojo pranešimo (pvz., ar incidentas išplito, ar sumažėjo, kokios nustatytos naujos jo priežastys arba kokių veiksmų imtasi problemai išspręsti). Bet kuriuo atveju buveinės valstybės narės kompetentingos institucijos prašymu mokėjimo paslaugų teikėjai turėtų nedelsdami parengti pranešimą.

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

2.14. Be to, mokėjimo paslaugų teikėjai kiekviename pranešime taip pat turėtų nurodyti kito informacijos atnaujinimo datą, kuri turėtų būti kuo ankstesnė ir jokiomis aplinkybėmis ne vėlesnė kaip po 3 darbo dienų. Jeigu mokėjimo paslaugų teikėjas negali kito informacijos atnaujinimo pateikti iki planuotos datos, jis turėtų susisiekti su kompetentinga institucija ir paaiškinti vėlavimo priežastis, pasiūlyti naują realistišką informacijos pateikimo terminą (ne ilgesnį kaip 3 darbo dienų) ir nusiųsti naują tarpinį pranešimą, kuriame atnaujinama tik informacija dėl planuojamos kito informacijos atnaujinimo datos.

2.15. Mokėjimo paslaugų teikėjai turėtų nusiųsti paskutinį 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.

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

Galutinis pranešimas

2.17. Mokėjimo paslaugų teikėjai turėtų nusiųsti 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 apytikrius vertinimus.

2.18. Mokėjimo paslaugų teikėjai daugiausia per 2 savaites nuo grįžimo prie įprastos verslo eigos kompetentingai institucijai turėtų pristatyti galutinį pranešimą. Mokėjimo paslaugų teikėjai, kuriems reikia, kad šis terminas būtų pratęstas (pvz., jeigu dar nėra faktinių duomenų apie poveikį), 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 aptikimo, jie turėtų siekti savo pirminiame pranešime pateikti informaciją, susijusią su pirminiu, paskutiniu tarpiniu ir galutiniu pranešimais.

2.20. Mokėjimo paslaugų teikėjai turėtų siekti į savo galutinius pranešimus įtraukti visą informaciją, t. y. i) faktinius duomenis apie poveikį, o ne apytikrius vertinimus (taip pat visą kitą atnaujintą informaciją, reikalingą šablono A ir B skirsniuose) ir ii) šablono C skirsnį, kuriame nurodoma pagrindinė priežastis, jeigu ji jau žinoma, ir apibendrinamos priemonės, kurių buvo imtasi arba bus imtasi 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 išsprendimo 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 statuso sumažinimo 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 (Elektroninių pinigų direktyva) 3 straipsnį; arba

ii. Europos bankininkystės priežiūros institucijų komiteto (EBPIK) gairėse dėl funkcijų perdavimo kredito įstaigoms.

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, įtraukti 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. Užtikrinti, kad trečioji šalis įvertintų incidento svarbumą kiekvienam paveiktam mokėjimo paslaugų teikėjui ir į konsoliduotąjį pranešimą įtrauktų tik tuos mokėjimo paslaugų teikėjus, kurių atžvilgiu incidentas klasifikuojamas kaip didelis. Be to, užtikrinti, kad, kilus abejonių, mokėjimo paslaugų teikėjas būtų įtrauktas į konsoliduotąjį pranešimą, kol nėra įrodymų, kad jis ten neturėtų būti įtrauktas.

e. 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) tuose laukeliuose, kur tai yra vienas iš variantų, naudotų intervalus, rodančius mažiausias ir aukščiausias vertes, pastebėtas ar apytikriai įvertintas skirtingų mokėjimo paslaugų teikėjų atžvilgiu.

f. Mokėjimo paslaugų teikėjai turėtų užtikrinti, kad trečioji šalis juos visą laiką informuotų apie visus aktualius incidento aspektus ir apie visą galimą trečiosios šalies bendravimą su kompetentinga institucija ir jo turinį, tačiau tik tiek, 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. Be to, mokėjimo paslaugų teikėjai turėtų užtikrinti, kad apie incidentą nebūtų pranešama du kartus – kad apie jį atskirai nepraneštų minėtasis mokėjimo paslaugų teikėjas ir dar kartą trečioji šalis.

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 keičiamasi

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 vietos institucijoms, nurodytoms taikant 5.1 gairę (t. y. *kitoms susijusioms vietos institucijoms*), bent jau tuo metu, kai gaunamas pirminis pranešimas (arba pranešimas, kuris paskatino keistis informacija) ir kai joms pranešama, kad sugrįžtama prie įprastos verslo eigos (t. y. kai gaunamas paskutinis tarpinis pranešimas).

6.2. Kompetentingos institucijos turėtų kitoms susijusioms 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 (pirminiame arba tarpiniame pranešime) mokėjimo paslaugų teikėjo nurodytą informaciją:

- incidento aptikimo datą ir laiką;
- incidento pradžios datą ir laiką;
- incidento išsprendimo arba tikėtino išsprendimo 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 kitomis susijusiomis 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 kitoms susijusioms 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 kitomis susijusiomis vietos institucijomis, konfidencialumą ir vientisumą ir kitoms susijusioms 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 keičiamasi

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 (t. y. pirminį, tarpinius ir galutinį pranešimus).

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 šablonai mokėjimo paslaugų teikėjams

CLASSIFICATION: RESTRICTED

Major Incident Report

☐ Initial report	within 4 hours after detection
☐ Intermediate report	maximum of 3 business days from previous report
☐ Last intermediate report	
☐ Final report	within 2 weeks after closing the incident
☐ Incident reclassified as non-major — Please explain:	

Report date	DD/MM/YYYY	Time	HH:MM
Incident identification number, if applicable (for interim and final reports)			

A - Initial report

A 1 - GENERAL DETAILS

Type of report					
Type of report	☐ Individual	☐ Consolidated			
Affected payment service provider (PSP)					
PSP name					
PSP unique identification number, if relevant					
PSP authorisation number					
Head of group, if applicable					
Home country					
Country/countries affected by the incident					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	
Reporting entity (complete this section if the reporting entity is not the affected PSP in case of delegated reporting)					
Name of the reporting entity					
Unique identification number, if relevant					
Authorisation number, if applicable					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	

A 2 - INCIDENT DETECTION and INITIAL CLASSIFICATION

Date and time of detection of the incident	DD/MM/YYYY, HH:MM		
The incident was detected by (1)		If Other, please explain:	
Please provide a short and general description of the incident (should you deem the incident to have an impact in other EU Member States(s), and if feasible within the applicable reporting deadlines, please provide a translation in English)			
What is the estimated time for the next update?	DD/MM/YYYY, HH:MM		

B - Intermediate report

B 1 - GENERAL DETAILS

Please provide a more DETAILED description of the incident. e.g. information on: - What is the specific issue? - How it happened - How did it develop - Was it related to a previous incident? - Consequences (in particular for payment service users) - Background of the incident detection - Areas affected - Actions taken so far - Service providers/ third party affected or involved - Crisis management started (internal and/or external (Central Bank Crisis management)) - PSP internal classification of the incident	
Date and time of beginning of the incident (if already identified)	DD/MM/YYYY, HH:MM
Incident status	☐ Diagnostics ☐ Recovery ☐ Repair ☐ Restoration
Date and time when the incident was restored or is expected to be restored	DD/MM/YYYY, HH:MM

B 2 - INCIDENT CLASSIFICATION & INFORMATION ON THE INCIDENT

Overall impact	☐ Integrity ☐ Confidentiality ☐ Continuity ☐ Availability ☐ Authenticity
Transactions affected [2]	Number of transactions affected — ☐ Actual figure ☐ Estimation As a % of regular number of transactions — ☐ Actual figure ☐ Estimation Value of transactions affected in EUR — ☐ Actual figure ☐ Estimation Comments:
Payment service users affected [3]	Number of payment service users affected — ☐ Actual figure ☐ Estimation As a %-of total payment service users — ☐ Actual figure ☐ Estimation
Service downtime[4]	Total service downtime DD:HH:MM — ☐ Actual figure ☐ Estimation
Economic impact [5]	Direct costs in EUR — ☐ Actual figure ☐ Estimation Indirect costs in EUR — ☐ Actual figure ☐ Estimation
High level of internal escalation	☐ YES ☐ YES, AND CRISIS MODE (OR EQUIVALENT) IS LIKELY TO BE CALLED UPON ☐ NO Describe the level of internal escalation of the incident, indicating if it has triggered or is likely to trigger a crisis mode (or equivalent) and if so, please describe
Other PSPs or relevant infrastructures potentially affected	☐ YES ☐ NO Describe how this incident could affect other PSPs and/or infrastructures
Reputational impact	☐ YES ☐ NO Describe how the incident could affect the reputation of the PSP (e.g. media coverage, potential legal or regulatory infringement, etc.)

B 3 - INCIDENT DESCRIPTION

Type of Incident	☐ Operational ☐ Security
Cause of incident	☐ Under investigation ☐ External attack ☐ Internal attack Type of attack: ☐ Distributed/Denial of Service (D/DoS) ☐ Infection of internal systems ☐ Targeted intrusion ☐ Other If Other, specify ☐ External events ☐ Human error ☐ Process failure ☐ System failure ☐ Other If Other, specify
Was the incident affecting you directly, or indirectly through a service provider?	☐ Directly ☐ Indirectly If indirectly, please provide the service provider's name

B 4 - INCIDENT IMPACT

Building(s) affected (Address), if applicable	
Commercial channels affected	☐ Branches ☐ Telephone banking ☐ Point of sale ☐ E-banking ☐ Mobile banking ☐ Other ☐ ATMs If Other, specify:
Payment services affected	☐ Cash placement on a payment account ☐ Credit transfers ☐ Money remittance ☐ Cash withdrawal from a payment account ☐ Direct debits ☐ Payment initiation services ☐ Operations required for operating a payment account ☐ Card payments ☐ Account information services ☐ Acquiring of payment instruments ☐ Issuing of payment instruments ☐ Other If Other, specify:
Functional areas affected	☐ Authentication/authorisation ☐ Clearing ☐ Indirect settlement ☐ Communication ☐ Direct settlement ☐ Other If Other, specify:
Systems and components affected	☐ Application/software ☐ Hardware ☐ Database ☐ Network/infrastructure ☐ Other If Other, specify:
Staff affected	☐ YES ☐ NO Describe how the incident could affect the staff of the PSP/service provider (e.g. staff not being able to reach the office to support customers, etc.)

B 5 - INCIDENT MITIGATION

Which actions/measures have been taken so far or are planned to recover from the incident?	
Has the Business Continuity Plan and/or Disaster Recovery Plan been activated? If so, when? If so, please describe	☐ YES ☐ NO DD/MM/YYYY, HH:MM
Has the PSP cancelled or weakened some controls because of the incident? If so, please explain	☐ YES ☐ NO

C - Final report	
If no intermediate report has been sent, please also complete section B	
C 1 - GENERAL DETAILS	
Please update the information from the intermediate report (summary): - additional actions/measures taken to recover from the incident - final remediation actions taken - root cause analysis - lessons learnt - addittional actions - any other relevant information	
Date and time of closing the incident	DD/MM/YYYY, HH:MM
If the PSP had to cancel or weaken some controls because of the incident, are the original controls back in place?	☐ YES ☐ NO
If so, please explain	
C 2 - ROOT CAUSE ANALYSIS AND FOLLOW-UP	
What was the root cause (if already known)? (possible to attach a file with detailed information)	
Main corrective actions/measures taken or planned to prevent the incident from happening again in the future, if already known	
C 3 - ADDITIONAL INFORMATION	
Has the incident been shared with other PSPs for information purposes?	☐ YES ☐ NO
If so, please provide details	
Has any legal action been taken against the PSP?	☐ YES ☐ NO
If so, please provide details	

Notes:

(1) Pull-down menu: payment service user; internal organisation; external organisation; none of the above

(2) Pull-down menu: > 10% of regular level of transactions and > EUR 100,000; > 25% of regular level of transactions or > EUR 5 milion; none of the above

(3) Pull-down menu: > 5,000 and > 10% payment service users; > 50,000 or > 25% payment service users; none of the above

(4) Pull-down menu: > 2 hours; < 2 hours

(5) Pull-down menu: > Max (0,1% Tier 1 capital, EUR 200,000) or > EUR 5 million; none of the above

CONSOLIDATED REPORT - LIST OF PSPs		
PSP Name	**PSP Unique Identification Number**	**PSP Authorisation number**

ŠABLONŲ PILDYMO NURODYMAI

Mokėjimo paslaugų teikėjai turėtų užpildyti aktualų šablono skirsnį, priklausomai nuo esamo pranešimo etapo: A skirsnį, kai pildomas pirminis pranešimas, B skirsnį, kai pildomi tarpiniai pranešimai, ir C skirsnį, kai pildomas galutinis pranešimas. Visi laukeliai yra privalomi, jeigu aiškiai nenurodyta kitaip.

Antraštė

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

Tarpinis pranešimas: tai yra ankstesnio (pirminio arba tarpinio) pranešimo apie tą patį incidentą atnaujinimas.

Paskutinis tarpinis pranešimas: juo buveinės valstybės narės kompetentinga institucija informuojama, kad įprasta veikla yra atkurta ir yra sugrįžta prie įprastos verslo eigos, taigi, daugiau tarpinių pranešimų nebus teikiama.

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

Incidentas perklasifikuotas į nedidelį: incidentas nebeatitinka didelio incidento kriterijų ir tikimasi, kad iki jo išsprendimo jis tų kriterijų nebeatitiks. Mokėjimo paslaugų teikėjai turėtų paaiškinti šio statuso sumažinimo motyvus.

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

Incidento identifikacinis numeris, jeigu taikytina (tarpiniam ir galutiniam pranešimui): numeris, kurį pirminio pranešimo pateikimo metu kompetentinga institucija priskiria siekdama unikaliai identifikuoti incidentą, jei taikytina (t. . jeigu kompetentinga institucija suteikia tokį numerį).

A. Pirminis pranešimas

A 1. Bendrieji duomenys

Pranešimo tipas:

Individualus: pranešimas susijęs su vienu mokėjimo paslaugų teikėju.

Konsoliduotasis: pranešimas susijęs su keliais mokėjimo paslaugų teikėjais, kurie naudojasi galimybe konsoliduotai teikti pranešimus. 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 mokėjimo paslaugų teikėjas: nurodomas incidentą patiriantis mokėjimo paslaugų teikėjas.

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

Mokėjimo paslaugų teikėjo unikalus identifikacinis numeris, jeigu aktualu: kiekvienoje valstybėje narėje naudojamas atitinkamas unikalus identifikacinis numeris mokėjimo paslaugų teikėjui identifikuoti, kurį mokėjimo paslaugų teikėjas nurodo, jeigu nepildomas laukelis *Mokėjimo paslaugų teikėjo leidimo numeris*.

Mokėjimo paslaugų teikėjo leidimo numeris: buveinės valstybės narės leidimo numeris.

Pagrindinis grupės subjektas subjektų grupių atveju, kaip apibrėžta 2015 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyvoje (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, nurodykite pagrindinio subjekto pavadinimą.

Buveinės šalis: valstybė narė, kurioje yra registruota mokėjimo paslaugų teikėjo buveinė; arba, jeigu mokėjimo paslaugų teikėjas pagal savo nacionalinę teisę registruotos buveinės neturi, tada – valstybė narė, kurioje yra jo pagrindinė buveinė.

Incidento paveikta šalis / šalys: šalis arba šalys**,** kuriose buvo jaučiamas incidento poveikis (pvz., paveikiami keli skirtingose šalyse esantys mokėjimo paslaugų teikėjo filialai). Ta šalis nebūtinai turi sutapti su buveinės valstybe nare.

Pagrindinis kontaktinis asmuo: paveikto mokėjimo paslaugų teikėjo darbuotojo – asmens, atsakingo už pranešimą apie incidentą, vardas ir pavardė arba, jeigu paveikto mokėjimo paslaugų teikėjo vardu pranešimus teikia trečioji šalis – 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. paštas.

Telefonas: telefono numeris, kuriuo prireikus galima paprašyti pateikti papildomus paaiškinimus. Tai gali būti asmeninis arba įmonės 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 mokėjimo paslaugų teikėjo vardu pranešimus teikia trečioji šalis – 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 galima paprašyti pateikti papildomus paaiškinimus. Tai gali būti asmeninis arba įmonės telefono numeris.

Pranešimą teikiantis subjektas: šis skirsnis turėtų būti pildomas, jeigu paveikto mokėjimo paslaugų teikėjo vardu pranešimų teikimo įpareigojimus vykdo trečioji šalis.

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

Unikalus identifikacinis numeris, jeigu aktualu: šalyje, kurioje yra trečioji šalis, naudojamas atitinkamas unikalus identifikacinis numeris pranešimą apie incidentą teikiančiam subjektui identifikuoti, kurį pranešimą teikiantis subjektas nurodo, jeigu nepildomas laukelis *Leidimo numeris*.

Leidimo numeris, jeigu taikytina: trečiosios šalies leidimo numeris šalyje, kurioje ji yra, kai taikytina.

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. paštas.

Telefonas: telefono numeris, kuriuo prireikus galima paprašyti pateikti papildomus paaiškinimus. Tai gali būti asmeninis arba įmonės 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 įmonės telefono numeris.

A 2. Incidento aptikimas ir pradinis klasifikavimas

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

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

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

Koks planuojamas kito informacijos atnaujinimo laikas?: nurodykite planuojamą kito informacijos atnaujinimo (tarpinio ar galutinio pranešimo) pateikimo datą ir laiką.

B. Tarpinis pranešimas

B 1. Bendrieji duomenys

Išsamesnis incidento aprašymas: aprašykite pagrindines incidento savybes, aptardami bent jau klausimyne išdėstytus aspektus (su kokia konkrečia problema mokėjimo paslaugų teikėjas susiduria, kaip ji kilo, kokia buvo jos raida, kaip ji galimai susijusi su ankstesniu incidentu, kokie jos padariniai, ypač mokėjimo paslaugų vartotojams, ir kt.).

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

Incidento statusas:

Diagnostika: incidento savybės ką tik nustatytos.

Atitaisymas: paveikti elementai perkonfigūruojami.

Regeneravimas: neveikiančių elementų būklė atstatoma iki paskutinės būklės, iki kurios ją galima atstatyti.

Atkūrimas: su mokėjimu susijusi paslauga vėl teikiama.

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.

B 2. Incidento klasifikavimas / informacija apie incidentą

Bendras poveikis: nurodykite, kokius aspektus paveikė incidentas. Galima pažymėti kelis langelius.

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

Prieinamumas: tokia su mokėjimu susijusių paslaugų ypatybė, kad prie jų gali gauti prieigą ir jomis naudotis mokėjimo paslaugų vartotojai.

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.

Tęstinumas: tokia ypatybė, kai organizacijos procesai, funkcijos ir turtas, reikalingi su mokėjimu susijusioms paslaugoms teikti, yra visapusiškai prieinami ir veikia iš anksto apibrėžtais prieinamais lygmenimis.

Paveiktos operacijos: mokėjimo paslaugų teikėjai 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. Mokėjimo paslaugų teikėjai turėtų nurodyti konkrečias šių kintamųjų vertes, kurios gali būti arba faktiniai duomenys, arba apytikriai vertinimai. Kelių mokėjimo paslaugų teikėjų vardu (t. y. konsoliduotai) pranešimus teikiantys subjektai vietoj to gali pateikti verčių intervalus, nurodydami mažiausias ir didžiausias vertes, pastebėtas arba apytikriai įvertintas į pranešimą įtrauktų mokėjimų paslaugų teikėjų grupėje, atskirdami jas brūkšneliu. 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, 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 mokėjimo paslaugų teikėjai šio skaičiaus nelaiko reprezentatyviu (pvz., dėl sezoniškumo), jie turėtų naudoti kitą, reprezentatyvesnį rodiklį ir laukelyje *Pastabos* kompetentingai institucijai nurodyti atitinkamą šio metodo loginį pagrindą.

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 apytikriai vertinimai. Kelių mokėjimo paslaugų teikėjų vardu (t. y. konsoliduotai) pranešimus teikiantys subjektai vietoj to gali pateikti verčių intervalus, nurodydami mažiausias ir didžiausias vertes, pastebėtas arba apytikriai įvertintas į pranešimą įtrauktų mokėjimų paslaugų teikėjų grupėje, atskirdami jas brūkšneliu. 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 taip pat įvertinti incidentą atsižvelgdami į savo pačių mokėjimo paslaugų vartotojus. 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.

Paslaugos neveikimo laikas: mokėjimo paslaugų teikėjai turėtų nurodyti, ar incidentas pasiekė arba, tikėtina, pasieks ribą, ir nurodyti atitinkamą skaičių – bendrą paslaugos neveikimo laiką. Mokėjimo paslaugų teikėjai turėtų nurodyti konkrečias šio kintamojo vertes, kurios gali būti arba faktiniai duomenys, arba apytikriai vertinimai. Kelių mokėjimo paslaugų teikėjų vardu (t. y. konsoliduotai) pranešimus teikiantys subjektai vietoj to gali pateikti verčių intervalą, nurodydami

mažiausias ir didžiausias vertes, pastebėtas arba apytikriai įvertintas į pranešimą įtrauktų mokėjimų paslaugų teikėjų grupėje, atskirdami jas brūkšneliu. 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 neveikimo 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, ir į nedarbo laiką bei techninės priežiūros laikotarpius. Jeigu mokėjimo paslaugų teikėjai negali nustatyti, kada nustojo būti vykdoma paslauga, paslaugos neveikimo laiką išimties tvarka jie turėtų pradėti skaičiuoti nuo neveikimo aptikimo momento.

Ekonominis poveikis: mokėjimo paslaugų teikėjai turėtų nurodyti, ar incidentas pasiekė arba, tikėtina, pasieks ribą, ir nurodyti atitinkamus duomenis – tiesiogines ir netiesiogines išlaidas. Mokėjimo paslaugų teikėjai turėtų nurodyti konkrečias šių kintamųjų vertes, kurios gali būti arba faktiniai duomenys, arba apytikriai vertinimai. Kelių mokėjimo paslaugų teikėjų vardu (t. y. konsoliduotai) pranešimus teikiantys subjektai vietoj to gali pateikti verčių intervalą, nurodydami mažiausias ir didžiausias vertes, pastebėtas arba apytikriai įvertintas į pranešimą įtrauktų mokėjimų paslaugų teikėjų grupėje, atskirdami jas brūkšneliu. 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.

> **Tiesioginės išlaidos:** incidento tiesiogiai padarytų nuostolių suma (eurais), įskaitant lėšas, reikalingas incidento padariniams pašalinti (pvz., nusavintoms lėšoms arba turtui grąžinti, aparatinei ir programinei įrangai pakeisti, sutartinių įsipareigojimų nesilaikymo mokesčiams sumokėti).
>
> **Netiesioginės išlaidos:** incidento netiesiogiai sukeltų nuostolių suma (eurais) (pvz., žalos atitaisymo ir kompensacijų vartotojams išlaidos, dėl praleistų verslo galimybių prarastos pajamos, galimos teisinės išlaidos).

Aukšto lygio vidinė sklaida: mokėjimo paslaugų teikėjai turėtų apsvarstyti, ar dėl poveikio su mokėjimu susijusioms paslaugoms apie incidentą ne pagal periodinių pranešimų procedūrą ir nuolat per visą incidento aktualumo laikotarpį bus pranešama vyriausiajam informacijos pareigūnui (arba panašiam pareigūnui). Jeigu pranešimų teikimas deleguojamas, vidinę sklaidą atlieka trečioji šalis. 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 mokėjimo paslaugų teikėjai arba susiję infrastruktūros objektai: mokėjimo paslaugų teikėjai turėtų įvertinti incidento poveikį finansų rinkai, kuri suprantama kaip finansų rinkos infrastruktūros objektai ir (arba) mokėjimo kortelių sistemos, kuriomis jie remiasi, taip pat kiti 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 visos finansų sistemos patikimumui. Mokėjimo paslaugų teikėjai turėtų nepamiršti įvairių aspektų, pvz., ar paveiktas elementas ir (arba) programinė įranga yra privati, 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: mokėjimo paslaugų teikėjai turėtų atsižvelgti į esamą arba, tikėtina, būsimą incidento pastebimumą 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) incidentas sukėlė pastebimą procesą ir todėl tikėtina, kad apie jį praneš arba jau pranešė žiniasklaida (įvertinant ne tik tradicinę žiniasklaidą, pvz., laikraščius, bet ir tinklaraščius, socialinius tinklus ir kt.), ii) nebuvo arba, tikėtina, nebus įvykdytos administracinės prievolės, iii) nebuvo arba, tikėtina, nebus laikomasi sankcijų arba iv) tokio pat pobūdžio incidentas jau yra įvykęs anksčiau.

B 3. Incidento aprašymas

Incidento tipas: nurodykite, ar, jūsų turimomis žiniomis, 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, autentiškumui ir (arba) tęstinumui.

Saugumas: prieiga prie mokėjimo paslaugų teikėjo turto, jo naudojimas, atskleidimas, sutrikdymas, modifikavimas ar sunaikinimas, turintis neigiamą poveikį su mokėjimu susijusių paslaugų vientisumui, prieinamumui, konfidencialumui, autentiškumui ir (arba) tęstinumui. Tai, be kita ko, gali įvykti, kai mokėjimo paslaugų teikėjas patiria kibernetinius išpuolius, netinkamai parengiamos ar įgyvendinamos saugumo politikos priemonės arba nepakankamai užtikrinamas fizinis saugumas.

Incidento priežastis: nurodykite incidento priežastį arba, jeigu ji dar nežinoma – labiausiai tikėtiną priežastį. Galima pažymėti kelis langelius.

Vyksta tyrimas: priežastis dar nenustatyta.

Išorinis išpuolis: priežasties šaltinis yra išorėje ir tyčia kėsinasi į mokėjimo paslaugų teikėją (pvz., kenkimo programinės įrangos išpuoliai).

Vidinis išpuolis: priežasties šaltinis yra viduje ir tyčia kėsinasi į mokėjimo paslaugų teikėją (pvz., sukčiavimas įstaigoje).

Išpuolio tipas:

DDoS ataka: bandymas padaryti internetinę paslaugą neprieinamą perkraunant ją srautu iš daugelio šaltinių.

Vidaus sistemų užkrėtimas: žalinga veikla, kuria rengiami išpuoliai prieš kompiuterines sistemas, bandant pasisavinti standžiojo disko vietą arba CPU laiką, prisijungti prie privačios informacijos, suardyti duomenis, siųsti šlamštą adresatams ir kt.

Tikslinis įsiskverbimas: sekimas, šnipinėjimas ir informacijos pasisavinimas kibernetinėje erdvėje.

Kita: bet koks kitas išpuolis, kurį mokėjimo paslaugų teikėjas gali būti patyręs tiesiogiai arba per paslaugos teikėją. Visų pirma, šis langelis turėtų būti pažymimas, jeigu buvo surengtas išpuolis prieš autorizavimo ir autentiškumo patvirtinimo procesą. Duomenys turėtų būti įvedami į tuščią teksto laukelį.

Išoriniai įvykiai: priežastis yra susijusi su įvykiais, kurių organizacija paprastai negali kontroliuoti (pvz., gaivalinėmis nelaimėmis, teisinėmis problemomis, verslo problemomis ir paslaugų priklausomybe).

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).

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 parengimu, vykdymu, elementais, specifikacijomis, integravimu ar sudėtingumu.

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

Ar incidentas jus paveikė tiesiogiai ar netiesiogiai per paslaugos teikėją?: incidentas mokėjimo paslaugų teikėją gali būti paveikęs tiesiogiai ar netiesiogiai per trečiąją šalį. Netiesioginio poveikio atveju nurodykite paslaugos teikėjo (-ų) pavadinimą.

B 4. Incidento poveikis

Paveiktas pastatas (adresas), jei taikytina: jeigu paveikiamas fizinis pastatas, nurodykite jo adresą.

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.

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 išdavimas: 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.

Informacijos apie sąskaitą 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.

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

Paveiktos funkcinės sritys: nurodykite incidento paveiktą mokėjimo proceso etapą arba etapus. Galima pažymėti kelis langelius.

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 arba vertybinius popierius.

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

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 mokėjimo paslaugų teikėjas.

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

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

Paveiktos sistemos ir elementai: nurodykite, kurią mokėjimo paslaugų teikėjo technologinės infrastruktūros dalį ar dalis paveikė incidentas. Galima pažymėti kelis langelius.

Taikomoji programa / programinė įranga: programos, operacinės sistemos ir kt., palaikančios mokėjimo paslaugų teikėjo mokėjimo paslaugų teikimą.

Duomenų bazė: duomenų struktūra, kurioje saugoma asmeninė ir mokėjimų informacija, reikalinga mokėjimo operacijoms atlikti.

Aparatinė įranga: fizinė technologinė įranga, vykdanti procesus ir (arba) sauganti duomenis, reikalingus mokėjimo paslaugų teikėjui su mokėjimais susijusiai veiklai vykdyti.

Tinklas / infrastruktūra: vieši arba privatūs telekomunikacijų tinklai, sudarantys sąlygas keistis duomenimis ir informacija mokėjimo proceso metu (pvz., internetas).

Kita: paveikta sistema ar elementas nėra nė vienas iš paminėtų variantų. Tuščiame teksto laukelyje turėtų būti pateikta papildoma informacija.

Paveikti darbuotojai: nurodykite, ar incidentas turėjo kokį nors poveikį mokėjimo paslaugų teikėjo darbuotojams, ir jeigu taip, pateikite informaciją tuščiame teksto laukelyje.

B 5. Incidento poveikio sumažinimas

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

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).

Ar dėl incidento mokėjimo paslaugų teikėjas atšaukė arba susilpnino kai kurias kontrolės priemones?: nurodykite, ar mokėjimo paslaugų teikėjas, siekdamas suvaldyti incidentą, turėjo panaikinti kai kurias kontrolės priemones (pvz., nustoti taikyti keturių akių principą), ir jeigu taip, tai nurodykite atitinkamas priežastis, kuriomis būtų pagrindžiamas kontrolės priemonių susilpninimas arba atšaukimas.

C. Galutinis pranešimas

C 1. Bendrieji duomenys

Tarpinio pranešimo informacijos atnaujinimas (santrauka): pateikite papildomą informaciją apie veiksmus, kurių imtasi incidentui neutralizuoti ir užtikrinti, kad jis nepasikartotų, pateikite pagrindinės priežasties analizę, nurodykite įgytą patirtį ir kt.

Incidento užbaigimo data ir laikas: nurodykite datą ir laiką, kai incidentas laikomas užbaigtu.

Ar grąžintos buvusios kontrolės priemonės?: jeigu mokėjimo paslaugų teikėjas dėl incidento turėjo atšaukti ar susilpninti kai kurias kontrolės priemones, nurodykite, ar tokios kontrolės priemonės yra grąžintos, ir tuščiame teksto laukelyje pateikite papildomą informaciją.

C 2. Pagrindinės priežasties analizė ir tolesni veiksmai

Kokia buvo pagrindinė priežastis, jeigu ji jau žinoma?: paaiškinkite, kokia yra incidento pagrindinė priežastis, arba, jeigu ji dar nežinoma – pateikite preliminarias pagrindinės priežasties analizės išvadas. Mokėjimo paslaugų teikėjas gali prisegti rinkmeną su išsamia informacija, jeigu mano, kad tai reikalinga.

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 incidentas jau aptartas su kitais mokėjimo paslaugų teikėjais informavimo 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).