EBA/GL/2017/10

19/12/2017

Pamatnostādnes

paziņošanai par būtiskiem incidentiem saskaņā ar Direktīvu (ES) 2015/2366 (MPD2)

1. Atbilstības un ziņošanas prasības

Pamatnostādņu statuss

1. Šis dokuments ietver pamatnostādnes, kas izdotas saskaņā ar Regulas (EK) Nr. 1093/2010 16. pantu[1]. Kompetentajām iestādēm un finanšu iestādēm saskaņā ar Regulas (EK) Nr. 1093/2010 16. panta 3. punktu jādara viss iespējamais, lai ievērotu šīs pamatnostādnes.

2. Pamatnostādnēs izklāstīts EBI skatījums uz atbilstošām uzraudzības praksēm Eiropas Finanšu uzraudzības sistēmā jeb par to, kā konkrētā jomā jāpiemēro Savienības tiesību akti. Kompetentajām iestādēm, kas minētas Regulas (ES) Nr. 1093/2010 4.panta 2.punktā, uz kurām attiecas šīs pamatnostādnes, tās būtu jāievēro, iekļaujot tās attiecīgi savā praksē (piemēram, veicot grozījumus savā tiesiskajā regulējumā vai uzraudzības procesos), tostarp gadījumos, ja pamatnostādnes ir paredzētas, galvenokārt, iestādēm.

Ziņošanas prasības

3. Saskaņā ar Regulas (ES) Nr. 1093/2010 16. panta 3. punktu kompetentajām iestādēm līdz 19/02/2018 jāpaziņo EBI, vai tās ievēro vai paredz ievērot šīs pamatnostādnes, vai jānorāda to neievērošanas iemesli. Ja šajā termiņā nebūs saņemts šāds paziņojums, EBI uzskatīs, ka kompetentās iestādes šos ieteikumus neievēro. Paziņojumi jāiesniedz, nosūtot EBI tīmekļa vietnē pieejamo veidlapu uz e-pasta adresi compliance@eba.europa.eu ar norādi „EBI/GL/2017/10". Paziņojumus nosūta personas, kas ir pilnvarotas kompetento iestāžu vārdā ziņot par prasību izpildi. Par jebkurām izmaiņām atbilstības statusā arī ir jāziņo EBI.

4. Paziņojumus publicēs EBI tīmekļa vietnē saskaņā ar 16. panta 3. punktu.

[1] Ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 1093/2010 (2010. gada 24. novembris), ar ko izveido Eiropas Uzraudzības iestādi (Eiropas Banku iestādi), tiek grozīts Lēmums Nr. 716/2009/EK un atcelts Komisijas Lēmums 2009/78/EK (OV L331, 15.12.2010., 12.lpp).

2. Priekšmets, piemērošanas joma un definīcijas

Priekšmets

5. Šīs pamatnostādnes izriet no pilnvarām, kas EBI piešķirtas 96. panta 3. punktā Eiropas Parlamenta un Padomes 2015. gada 25. novembra Direktīvā (ES) 2015/2366 par maksājumu pakalpojumiem iekšējā tirgū, ar ko groza Direktīvas 2002/65/EK, 2009/110/EK un 2013/36/EK un Regulu (ES) Nr. 1093/2010 un atceļ Direktīvu 2007/64/EK (pārskatītā Maksājumu pakalpojumu direktīva, MPD2).

6. Jo īpaši šajās pamatnostādnēs ir precizēti kritēriji, pēc kuriem maksājumu pakalpojumu sniedzējiem ir jāklasificē būtiski operacionālie vai drošības incidenti, kā arī formāts un procedūras, kas tiem jāievēro, paziņojot par šādiem incidentiem piederības dalībvalsts kompetentajai iestādei, kā noteikts minētās direktīvas 96. panta 1. punktā.

7. Šajās pamatnostādnēs ir arī noteikts, kā šīs kompetentās iestādes izvērtē incidenta būtiskumu un incidenta ziņojumu elementus, kurus saskaņā ar minētās direktīvas 96. panta 2. punktu tās dara zināmus citām valsts iestādēm.

8. Turklāt šajās pamatnostādnēs ir izskatīts jautājums par EBI un ECB informēšanu par būtiskajiem paziņoto incidentu elementiem, lai sekmētu vienotu un konsekventu pieeju.

Piemērošanas joma

9. Šīs pamatnostādnes piemēro attiecībā uz būtisku operacionālo vai drošības incidentu klasifikāciju un paziņošanu par tiem saskaņā ar Direktīvas (ES) 2015/2366 96. pantu.

10. Šīs pamatnostādnes piemēro attiecībā uz visiem incidentiem, kuri atbilst "būtiska operacionālā vai drošības incidenta" definīcijai, kas aptver gan ārējus, gan iekšējus notikumus, kuri var būt ļaunprātīgi vai nejauši.

11. Šīs pamatnostādnes piemēro arī gadījumos, kad būtisks operacionālais vai drošības incidents rodas ārpus Savienības (piem., kad incidents rodas mātes sabiedrībā vai meitas sabiedrībā, kas atrodas ārpus Savienības) un ietekmē maksājumu pakalpojumus, ko sniedz Savienībā esošs maksājumu pakalpojumu sniedzējs vai nu tieši (ar maksājumu saistītu pakalpojumu sniedz ietekmētais uzņēmums, kas nav Savienības uzņēmums), vai netieši (incidenta rezultātā maksājumu pakalpojumu sniedzēja spēja turpināt veikt maksājumu darbības ir apdraudēta kādā citā veidā).

Adresāti

12. Pirmā pamatnostādņu kopuma (4. nodaļa) adresāts ir maksājumu pakalpojumu sniedzēji (MPS), kā definēts Direktīvas (ES) 2015/2366 4. panta 11) punktā un kā minēts Regulas (ES) Nr. 1093/2010 4. panta 1. punktā.

13. Otrā un trešā pamatnostādņu kopuma (5. un 6. nodaļa) adresāts ir kompetentās iestādes, kā definēts Regulas (ES) Nr. 1093/2010 4. panta 2. punkta i) apakšpunktā.

Definīcijas

14. Ja nav norādīts citādi, terminiem, kas lietoti un definēti Direktīvā (ES) 2015/2366, tāda pati nozīme ir arī šajās pamatnostādnēs. Papildus šajās pamatnostādnēs piemēro šādas definīcijas:

Operacionālais vai drošības incidents	Vienreizējs notikums vai vairāki saistīti notikumi, kurus maksājumu pakalpojumu sniedzējs nav plānojis un kuri negatīvi ietekmē vai, iespējams, ietekmēs ar maksājumiem saistīto pakalpojumu integritāti, pieejamību, konfidencialitāti, autentiskumu un/vai nepārtrauktību.
Integritāte	Īpašība, kas nozīmē, ka tiek garantēta aktīvu (arī datu) precizitāte un pilnīgums.
Pieejamība	Īpašība, kas nozīmē, ka ar maksājumiem saistītie pakalpojumi ir pieejami maksājumu pakalpojumu lietotājiem un viņi var tos izmantot.
Konfidencialitāte	Īpašība, kas nozīmē, ka informācija nav pieejama vai nav izpaužama personām, organizācijām vai procesiem, kuriem nav atbilstoša pilnvarojuma.
Autentiskums	Īpašība, kas nozīmē, ka izcelsme atbilst apgalvotajam.
Nepārtrauktība	Īpašība, kas nozīmē, ka organizācijas procesi, uzdevumi un aktīvi, kas nepieciešami, lai nodrošinātu ar maksājumu saistītus pakalpojumus, ir pilnībā pieejami un darbojas pieņemamos, iepriekš noteiktos līmeņos.
Ar maksājumiem saistīti pakalpojumi	Kāds no pakalpojumu darbības veidiem MPD2 4. panta 3) punkta izpratnē, kā arī visi tehniskā atbalsta uzdevumi, kas nepieciešami maksājumu pakalpojumu pareizai sniegšanai.

3. Īstenošana

Piemērošanas datums

15. Šīs pamatnostādnes ir piemērojamas no 2018. gada 13. janvāra.

4. Pamatnostādnes, kuru adresāts ir maksājumu pakalpojumu sniedzēji un kas attiecas uz paziņošanu viņu piederības dalībvalsts kompetentajai iestādei par būtiskiem operacionālajiem vai drošības incidentiem

1. pamatnostādne. Būtiska incidenta klasifikācija

1.1. Maksājumu pakalpojumu sniedzējiem (MPS) kā būtiski ir jāklasificē tādi operacionālie vai drošības incidenti, kuri atbilst

a. vienam vai vairākiem kritērijiem "augstākas ietekmes līmenī" vai

b. trim vai vairākiem kritērijiem "zemākas ietekmes līmenī",

kā noteikts 1.4. pamatnostādnē un atbilstoši šajās pamatnostādnēs izklāstītajam novērtējumam.

1.2. Maksājumu pakalpojumu sniedzējiem ir jānovērtē operacionālais vai drošības incidents atbilstoši šādiem kritērijiem un indikatoriem, uz kuriem tie ir balstīti:

i. ietekmētie darījumi

Maksājumu pakalpojumu sniedzējiem ir jānosaka ietekmēto darījumu kopējā vērtība, kā arī apdraudēto maksājumu skaits procentos no to maksājumu darījumu ierastā līmeņa, kurus veic, izmantojot ietekmētos maksājumu pakalpojumus.

ii. ietekmētie maksājumu pakalpojumu lietotāji

Maksājumu pakalpojumu sniedzējiem ir jānosaka ietekmēto maksājumu pakalpojuma lietotāju skaits gan absolūtā izteiksmē, gan procentos no maksājumu pakalpojumu lietotāju kopējā skaita.

iii. pakalpojuma dīkstāve

Maksājumu pakalpojumu sniedzējiem ir jānosaka laikposms, kurā pakalpojums, visticamāk, nebūs pieejams maksājumu pakalpojumu lietotājam vai kurā maksājumu pakalpojumu sniedzējs nevarēs izpildīta maksājuma uzdevumu MPD2 4. panta 13) punkta izpratnē.

iv. ekonomiskā ietekme

Maksājumu pakalpojumu sniedzējiem ir holistiski jānosaka monetārās izmaksas, kas ir saistītas ar incidentu, un ir jāņem vērā gan absolūtais skaitlis, gan attiecīgā gadījumā šo

izmaksu relatīvā nozīme attiecībā uz maksājumu pakalpojumu sniedzēja lielumu (t. i., maksājumu pakalpojumu sniedzēja 1. līmeņa pamatkapitālu).

v. augsts iekšējās eskalācijas līmenis

Maksājumu pakalpojumu sniedzējiem ir jānosaka, vai par šo incidentu ir ziņots vai tiks ziņots to izpilddirektoriem.

vi. citi potenciāli ietekmētie maksājumu pakalpojumu sniedzēji vai attiecīgās infrastruktūras

Maksājumu pakalpojumu sniedzējiem ir jānosaka sistēmiskās sekas, kādas, visticamāk, būs šim incidentam, t. i., tā potenciāls papildus sākotnēji ietekmētajam maksājumu pakalpojumu sniedzējam ietekmēt arī citus maksājumu pakalpojumu sniedzējus, finanšu tirgus infrastruktūras un/vai maksājumu karšu shēmas.

vii. ietekme uz reputāciju

Maksājumu pakalpojumu sniedzējiem ir jānosaka, kā šis incidents var samazināt lietotāju uzticēšanos pašam maksājumu pakalpojumu sniedzējam un vispārīgi — pamatpakalpojumam vai tirgum kopumā.

1.3. Maksājumu pakalpojumu sniedzējiem ir jāaprēķina indikatoru vērtība atbilstoši šādai metodoloģijai:

i. ietekmētie darījumi

Parasti maksājumu pakalpojumu sniedzējiem jēdziens "ietekmētie darījumi" ir jāizprot kā visi pašmāju un pārrobežu darījumi, kurus incidents ir tieši vai netieši ietekmējis vai, visticamāk, ietekmēs, jo īpaši tie darījumi, kurus nav bijis iespējams uzsākt vai apstrādāt, kuriem tika izmainīts maksājuma ziņojuma saturs un kuri tika pasūtīti krāpnieciski (neatkarīgi no tā, vai līdzekļi ir atgūti vai nav).

Turklāt maksājumu pakalpojumu sniedzējiem jēdziens "maksājumu darījumu ierastais līmenis" ir jāizprot kā to ikdienas pašmāju un pārrobežu maksājumu darījumu vidējais skaits gadā, kurus veic, izmantojot tos pašus maksājumu pakalpojumus, kurus ietekmēja incidents, par atsauces periodu aprēķiniem ņemot iepriekšējo gadu. Ja maksājumu pakalpojumu sniedzēji neuzskata, ka šis rādītājs ir reprezentatīvs (piem., sezonalitātes dēļ), viņiem tā vietā ir jāizmanto cits, reprezentatīvāks rādītājs un atbilstošajā veidnes laukā (sk. 1. pielikumu) ir jāsniedz kompetentajai iestādei šādas pieejas pamatojums.

ii. ietekmētie maksājumu pakalpojumu lietotāji

Maksājumu pakalpojumu sniedzējiem ir jāizprot jēdziens "ietekmētie maksājumu pakalpojumu lietotāji" kā visi klienti (pašmāju un ārzemju, patērētāji un uzņēmumi), kuriem ar ietekmēto maksājumu pakalpojumu sniedzēju ir noslēgts līgums, kas tiem piešķir piekļuvi ietekmētajam maksājumu pakalpojumam, un kuri ir cietuši vai, visticamāk, cietīs no incidenta sekām. Maksājumu pakalpojumu sniedzējiem aplēses ir jābalsta uz iepriekšējām norisēm, lai noteiktu to maksājumu pakalpojumu lietotāju skaitu, kuri, iespējams, incidenta pastāvēšanas laikā ir izmantojuši minēto maksājumu pakalpojumu.

Grupu gadījumā katram maksājumu pakalpojumu sniedzējam ir jāņem vērā tikai paša maksājumu pakalpojumu lietotāji. Ja maksājumu pakalpojumu sniedzējs piedāvā darbības pakalpojumus citiem, šim maksājumu pakalpojumu sniedzējam ir jāņem vērā tikai savi maksājumu pakalpojumu lietotāji (ja tādi ir) un tiem maksājumu pakalpojumu sniedzējiem, kuri saņem minētos darbības pakalpojumus, ir jānovērtē incidents saistībā ar saviem maksājumu pakalpojumu lietotājiem.

Turklāt maksājumu pakalpojumu sniedzējiem kā kopējais maksājumu pakalpojumu lietotāju skaits ir jāpieņem to pašmāju un pārrobežu maksājumu pakalpojumu lietotāju kopskaits, ar kuriem incidenta laikā ir bijušas noslēgtas līgumattiecības (vai arī visnesenākais pieejamais rādītājs) un kuriem ir pieeja ietekmētajam maksājumu pakalpojumam neatkarīgi no to lieluma un no tā, vai tie ir uzskatāmi par aktīviem vai pasīviem maksājumu pakalpojumu lietotājiem.

iii. pakalpojuma dīkstāve

Maksājumu pakalpojumu sniedzējiem ir jāņem vērā laikposms, kurā jebkurš uzdevums, process vai kanāls, kas ir saistīts ar maksājumu pakalpojumu sniegšanu, nav vai, visticamāk, nebūs pieejams, tādējādi liedzot i) uzsākt un/vai veikt maksājumu pakalpojumu un/vai ii) piekļūt maksājumu kontam. Maksājumu pakalpojumu sniedzējiem pakalpojuma dīkstāve ir jāaprēķina no brīža, kad dīkstāve sākas, un viņiem ir jāņem vērā gan laikposmi, kuros tie ir atvērti pakalpojumu darbībai, kas nepieciešama maksājumu pakalpojumu izpildei, gan arī laikposmi ārpus darba laika un uzturēšanas laikposmi, ja tas ir atbilstoši un piemērojami. Ja maksājumu pakalpojumu sniedzēji nevar noteikt, kad pakalpojuma dīkstāve ir sācies, viņiem izņēmuma kārtā pakalpojuma dīkstāve ir jāaprēķina no brīža, kad tas tika konstatēts.

iv. ekonomiskā ietekme

Maksājumu pakalpojumu sniedzējiem ir jāņem vērā izmaksas, kas var būt gan tieši, gan netieši saistītas ar incidentu. Cita starpā maksājumu pakalpojumu sniedzējiem ir jāņem vērā ekspropriētie līdzekļi vai aktīvi, aparatūras vai programmatūras aizstāšanas izmaksas, citas tiesu vai atlīdzināšanas izmaksas, maksas, kas piemērotas līgumsaistību neizpildes dēļ, sankcijas, ārējas saistības un zaudētie ieņēmumi. Attiecībā uz netiešajām izmaksām maksājumu pakalpojumu sniedzējiem ir jāņem vērā tikai tās izmaksas, kas jau ir zināmas vai, visticamāk, radīsies.

v. *augsts iekšējās eskalācijas līmenis*

Maksājumu pakalpojumu sniedzējiem ir jāizvērtē, vai par incidentu tādēļ, kā tas ietekmē ar maksājumiem saistītus pakalpojumus, (visticamāk) tiks informēts informācijas direktors (vai līdzīga līmeņa amatpersona) ārpus periodiskās ziņošanas procedūras un nepārtraukti incidenta pastāvēšanas laikā. Tāpat maksājumu pakalpojumu sniedzējiem ir jāapsver, vai incidents ietekmē ar maksājumiem saistītus pakalpojumus tā, ka tā rezultātā ir noteikts vai, visticamāk, tiks noteikts krīzes režīms.

vi. *citi potenciāli ietekmētie maksājumu pakalpojumu sniedzēji vai attiecīgās infrastruktūras*

Maksājumu pakalpojumu sniedzējiem ir jānovērtē incidenta ietekme uz finanšu tirgu, ar ko saprot finanšu tirgus infrastruktūras un/vai karšu maksājumu shēmas, kuras atbalsta tos un

citus maksājumu pakalpojumu sniedzējus. It īpaši maksājumu pakalpojumu sniedzējiem ir jānovērtē, vai incidents (visticamāk) tiks replicēts citiem maksājumu pakalpojumu sniedzējiem neatkarīgi no tā, vai tas ir ietekmējis vai, visticamāk, ietekmēs finanšu tirgus infrastruktūru nevainojamu funkcionēšanu un vai tas ir negatīvi ietekmējis vai, visticamāk, negatīvi ietekmēs finanšu sistēmas stabilu darbību kopumā. Maksājumu pakalpojumu sniedzējiem ir jāņem vērā dažādas dimensijas, piemēram, vai ietekmētais komponents/programmatūra ir patentēti vai vispārpieejami, vai negatīvi ietekmētais tīkls ir iekšējs vai ārējs un vai maksājumu pakalpojumu sniedzējs ir pārtraucis vai, visticamāk, pārtrauks pildīt savus pienākumus tajās finanšu tirgus infrastruktūrās, kurās tas ir dalībnieks.

vii. *ietekme uz reputāciju*

Maksājumu pakalpojumu sniedzējiem ir jāņem vērā atpazīstamības līmenis, kuru (pēc to rīcībā esošās informācijas) incidents ir panācis vai, visticamāk, panāks tirgū. It īpaši maksājumu pakalpojumu sniedzējiem ir jāņem vērā varbūtība, ka incidents izraisīs kaitējumu sabiedrībai, kā piemērots rādītājs tā potenciālam ietekmēt viņu reputāciju. Maksājumu pakalpojumu sniedzējiem ir jāņem vērā, vai i) incidents ir ietekmējis redzamu procesu un tāpēc, visticamāk, tiks apskatīts vai jau ir apskatīts plašsaziņas līdzekļos (ņemot vērā ne tikai tradicionālos plašsaziņas līdzekļus, piem., laikrakstus, bet arī emuārus, sociālos tīklus utt.), ii) nav ievērotas vai, visticamāk, netiks ievērotas normatīvās prasības, iii) sankcijas ir vai, visticamāk, tiks pārkāptas vai iv) iepriekš ir noticis tāda paša veida incidents.

1.4. Maksājumu pakalpojumu sniedzējiem ir jānovērtē incidents, attiecībā uz katru atsevišķo kritēriju nosakot, vai līdz incidenta atrisināšanai ir sasniegtas vai, visticamāk, tiks sasniegtas attiecīgās robežvērtības, kas noteiktas 1. tabulā.

1. tabula. Robežvērtības

Kritērijs	Zemāks ietekmes līmenis	Augstāks ietekmes līmenis
Ietekmētie darījumi	> 10 % no maksājumu pakalpojumu sniedzēja ierastā darījumu līmeņa (darījumu skaita ziņā) **un** > 100 000 EUR	> 25 % no maksājumu pakalpojumu sniedzēja ierastā darījumu līmeņa (darījumu skaita ziņā) **vai** > 5 miljoni EUR
Ietekmētie maksājumu pakalpojumu lietotāji	> 5000 **un** > 10 % no maksājumu pakalpojumu sniedzēja maksājumu pakalpojumu lietotājiem	> 50 000 **vai** > 25 % no maksājumu pakalpojumu sniedzēja maksājumu pakalpojumu lietotājiem
Pakalpojuma dīkstāve	> 2 stundas	Nav piemērojams
Ekonomiskā ietekme	Nav piemērojams	> maks. (0,1 % no 1. līmeņa pamatkapitāla*, 200 000 EUR) **vai** > 5 miljoni EUR
Augsts iekšējās eskalācijas līmenis	Jā	Jā, un, iespējams, tiks noteikts krīzes (vai tai pielīdzināms) režīms
Citi potenciāli ietekmētie maksājumu pakalpojumu sniedzēji vai attiecīgās infrastruktūras	Jā	Nav piemērojams
Ietekme uz reputāciju	Jā	Nav piemērojams

*1. līmeņa pamatkapitāls, kā noteikts 25. pantā Eiropas Parlamenta un Padomes 2013. gada 26. jūnija Regulā (ES) Nr. 575/2013 par prudenciālajām prasībām attiecībā uz kredītiestādēm un ieguldījumu brokeru sabiedrībām, un ar ko groza Regulu (ES) Nr. 648/2012.

1.5. Maksājumu pakalpojumu sniedzējiem ir jāpielieto aplēses, ja tiem nav faktisku datu, ar ko pamatot savus slēdzienus, neatkarīgi no tā, vai līdz incidenta atrisināšanai ir sasniegta vai, visticamāk, tiks sasniegta konkrēta robežvērtība (piem., tas var notikt sākotnējās izmeklēšanas fāzē).

1.6. Maksājumu pakalpojumu sniedzējiem pastāvīgi incidenta pastāvēšanas laikā ir jāveic šis novērtējums, lai identificētu iespējamas statusa izmaiņas augšup (no nebūtiska uz būtisku) vai lejup (no būtiska uz nebūtisku).

2. pamatnostādne. Paziņošanas process

2.1. Maksājumu pakalpojumu sniedzējiem ir jāapkopo visa būtiskā informācija, jāsagatavo ziņojums par incidentu, izmantojot 1. pielikumā doto formu, un tas jāiesniedz savas piederības dalībvalsts kompetentajai iestādei. Maksājumu pakalpojumu sniedzējiem ir jāaizpilda minētā forma atbilstoši 1. pielikumā dotajiem norādījumiem.

2.2. Maksājumu pakalpojumu sniedzējiem ir jāizmanto tā pati forma, lai informētu kompetento iestādi incidenta pastāvēšanas laikā (t. i., lai sagatavotu sākotnējo, starposma un noslēguma ziņojumu, kā aprakstīts 2.7. līdz 2.21. punktā). Maksājumu pakalpojumu sniedzējiem ir

jāaizpilda forma pakāpeniski, pēc iespējas papildinot to ar jaunu informāciju, kas kļūst pieejama iekšējās izmeklēšanas gaitā.

2.3. Maksājumu pakalpojumu sniedzējiem savas piederības dalībvalsts kompetentajai iestādei attiecīgajā gadījumā ir jāiesniedz arī tās informācijas eksemplārs, kuru tas sniedza (vai sniegs) saviem lietotājiem, kā noteikts MPD2 96. panta 1. punkta 2. rindkopā, tiklīdz tā kļūst pieejama.

2.4. Maksājumu pakalpojumu sniedzējiem ir jāsniedz savas piederības dalībvalsts kompetentajai iestādei jebkāda papildinformācija, ja tā pieejama un ir uzskatāms, ka tā ir būtiska kompetentajai iestādei, pievienojot standarta formai papildu dokumentāciju kā vienu vai vairākus pielikumus.

2.5. Maksājumu pakalpojumu sniedzējiem ir jāveic papildu pasākumi, atbildot uz savas piederības dalībvalsts kompetentās iestādes jebkādiem pieprasījumiem sniegt papildinformāciju vai skaidrojumu saistībā ar jau iesniegtu dokumentāciju.

2.6. Maksājumu pakalpojumu sniedzējiem vienmēr ir jāsaglabā tās informācijas konfidencialitāte un integritāte, ar kuru tie apmainās ar savas piederības dalībvalsts kompetento iestādi, kā arī ir pienācīgi jāapstiprina savs autentiskums savas piederības dalībvalsts kompetentajai iestādei.

Sākotnējais ziņojums

2.7. Maksājumu pakalpojumu sniedzējiem ir jāiesniedz savas piederības dalībvalsts kompetentajai iestādei sākotnējais ziņojums, kad pirmoreiz ir konstatēts būtisks operacionālais vai drošības incidents.

2.8. Maksājumu pakalpojumu sniedzējiem sākotnējais ziņojums ir jānosūta kompetentajai iestādei 4 stundās pēc tam, kad pirmoreiz ir konstatēts būtisks operacionālais vai drošības incidents, vai, ja ir zināms, ka šajā laikā kompetentās iestādes ziņošanas kanāli nav pieejami vai nedarbojas, — tiklīdz tie atkal kļūst pieejami / atsāk darboties.

2.9. Maksājumu pakalpojumu sniedzējiem ir jāiesniedz sākotnējais ziņojums savas piederības dalībvalsts kompetentajai iestādei arī tad, ja iepriekš par nebūtisku atzīts incidents kļūst par būtisku incidentu. Šajā konkrētajā gadījumā maksājumu pakalpojumu sniedzējiem sākotnējais ziņojums ir jānosūta kompetentajai iestādei, tiklīdz ir konstatēta statusa maiņa, vai, ja ir zināms, ka tajā laikā kompetentās iestādes ziņošanas kanāli nav pieejami vai nedarbojas, — tiklīdz tie atkal kļūst pieejami / atsāk darboties.

2.10. Maksājumu pakalpojumu sniedzējiem sākotnējā ziņojumā ir jāiekļauj nosaukuma līmeņa informācija (t. i., formas A sadaļa), norādot dažas incidenta pamatiezīmes un tā paredzamās sekas, pamatojoties uz informāciju, kas ir pieejama nekavējoties pēc tam, kad incidents ir konstatēts vai pārklasificēts. Ja faktiski dati nav pieejami, maksājumu pakalpojumu sniedzējiem ir jāizmanto aplēses. Maksājumu pakalpojumu sniedzējiem sākotnējā ziņojumā

ir jānorāda arī datums, kad tiks sniegts nākamais atjauninājums, un tam ir jābūt tik drīz, cik vien iespējams, bet nekādā gadījumā ne vēlāk kā pēc 3 darba dienām.

Starpposma ziņojums

2.11. Maksājumu pakalpojumu sniedzējiem ir jāiesniedz starpposma ziņojumi ik reizi, kad tie uzskata, ka ir noticis būtisks statusa atjauninājums, un vismaz līdz nākamā atjauninājuma datumam, kas norādīts iepriekšējā ziņojumā (vai nu sākotnējā ziņojumā, vai iepriekšējā starpposma ziņojumā).

2.12. Maksājumu pakalpojumu sniedzējiem ir jāiesniedz kompetentajai iestādei pirmais starpposma ziņojums, kurā ir ietverta detalizētāka informācija par incidentu un tā sekām (formas B sadaļa). Turklāt maksājumu pakalpojumu sniedzējiem ir jāsagatavo papildu starpposma ziņojumi, aktualizējot informāciju, kas jau ir iesniegta formas A un B sadaļā, vismaz tad, kad pēc iepriekšējā paziņojuma tiem kļūst zināma jauna būtiska informācija vai notiek būtiskas izmaiņas (piem., vai incidents ir eskalējies vai samazinājies, informācija par jauniem identificētiem cēloņiem vai veiktajām darbībām, lai problēmu novērstu). Jebkurā gadījumā maksājumu pakalpojumu sniedzējiem starpposma ziņojums ir jāsagatavo pēc savas piederības dalībvalsts kompetentās iestādes pieprasījuma.

2.13. Tāpat kā sākotnējo ziņojumu gadījumā, ja nav pieejami faktiski dati, maksājumu pakalpojumu sniedzējiem ir jāizmanto aplēses.

2.14. Turklāt maksājumu pakalpojumu sniedzējiem katrā ziņojumā ir jānorāda arī datums, kad tiks sniegts nākamais atjauninājums, un tam ir jābūt tik drīz, cik vien iespējams, bet nekādā gadījumā ne vēlāk kā pēc 3 darba dienām. Ja maksājumu pakalpojumu sniedzējs nevar ievērot paredzamo nākamā atjauninājuma datumu, tam ir jāsazinās ar kompetento iestādi, lai paskaidrotu kavēšanās iemeslus, piedāvātu jaunu, izpildāmu iesniegšanas termiņu (ne vēlāk kā pēc 3 darba dienām) un nosūtītu jaunu starpposma ziņojumu, tajā aktualizējot tikai informāciju par paredzamo nākamā atjauninājuma datumu.

2.15. Maksājumu pakalpojumu sniedzējiem pēdējais starpposma ziņojums ir jānosūta tad, kad ir atjaunotas ierastās darbības un pakalpojumu darbība norit normāli, informējot par to kompetento iestādi. Maksājumu pakalpojumu sniedzējiem ir jāuzskata, ka pakalpojumu darbība atkal norit normāli, ja darbība/funkcijas ir atjaunotas tādā pašā pakalpojumu/nosacījumu līmenī, kā to noteicis maksājumu pakalpojumu sniedzējs vai kā noteikts ārējā nolīgumā par pakalpojumu līmeni (*SLA*) attiecībā uz apstrādes laikiem, darbspēju, drošības prasībām utt., un ja vairs netiek īstenoti ārkārtas pasākumi.

2.16. Ja pakalpojumu darbība atgriežas ierastajā ritmā, pirms ir pagājušas 4 stundas kopš incidenta konstatēšanas, maksājumu pakalpojumu sniedzējiem ir jācenšas vienlaicīgi iesniegt gan sākotnējo, gan pēdējo starpposma ziņojumu (t. i., aizpildot formas A un B sadaļu) pirms 4 stundu termiņa beigām.

Noslēguma ziņojums

2.17. Maksājumu pakalpojumu sniedzējiem ir jānosūta noslēguma ziņojums, kad ir veikta pirmcēloņa analīze (neatkarīgi no tā, vai seku mazināšanas pasākumi jau ir veikti un vai ir identificēts galīgais pirmcēlonis) un ir pieejami faktiskie dati, lai aizstātu aplēses.

2.18. Maksājumu pakalpojumu sniedzējiem noslēguma ziņojums kompetentajai iestādei ir jāiesniedz ne vēlāk kā 2 nedēļās pēc tam, kad var uzskatīt, ka pakalpojumu darbība ir atgriezusies ierastajā gaitā. Maksājumu pakalpojumu sniedzējiem, kuriem ir nepieciešams šā termiņa pagarinājums (piem., ja vēl nav pieejamas faktiskie ietekmes rādītāji), ir jāsazinās ar kompetento iestādi, pirms ir iestājies minētais termiņš, un ir jānorāda pienācīgs kavējuma pamatojums, kā arī jauns paredzamais noslēguma ziņojuma datums.

2.19. Ja maksājumu pakalpojumu sniedzēji var iesniegt visu informāciju, kas nepieciešama noslēguma ziņojumā (t. i., formas C sadaļā), 4 stundās kopš incidenta konstatēšanas, tiem ir jācenšas sākotnējā ziņojumā iesniegt informāciju, kas saistīta ar sākotnējo, pēdējo starpposma un noslēguma ziņojumu.

2.20. Maksājumu pakalpojumu sniedzējiem noslēguma ziņojumos ir jācenšas iekļaut pilnīgu informāciju, t. i., i) faktiskos rādītājus par ietekmi, nevis aplēses (kā arī citus atjauninājumus, kas nepieciešami formas A un B sadaļā), un ii) formas C sadaļu, kurā norāda pirmcēloni, ja tas ir jau noskaidrots, kā arī kopsavilkumu par pasākumiem, kuri ir jau pieņemti vai kurus ir plānots pieņemt, lai likvidētu problēmu un novērstu tās atkārtošanos turpmāk.

2.21. Maksājumu pakalpojumu sniedzējiem ir jānosūta noslēguma ziņojums arī tad, ja incidenta nepārtrauktas novērtēšanas rezultātā tie konstatē, ka incidents, par kuru jau ir paziņots, vairs neatbilst kritērijiem, pēc kuriem to atzīst par būtisku, un nav sagaidāms, ka tas atbildīs minētajiem kritērijiem, pirms incidents tiks atrisināts. Šajā gadījumā maksājumu pakalpojumu sniedzējiem noslēguma ziņojums ir jānosūta, tiklīdz šis apstāklis ir konstatēts, bet jebkurā gadījumā — līdz paredzētajam nākamā ziņojuma datumam. Šajā konkrētajā gadījumā tā vietā, lai aizpildītu formas C sadaļu, maksājumu pakalpojumu sniedzējiem ir jāatzīmē lodziņš “incidents pārklasificēts kā nebūtisks” un ir jāpaskaidro iemesli, kas pamato šādu pazemināšanu.

3. pamatnostādne. Deleģētā un konsolidētā paziņošana

3.1. Ja kompetentā iestāde to pieļauj, maksājumu pakalpojumu sniedzēji, kas saskaņā ar MPD2 vēlas deleģēt ziņošanas pienākumus trešai personai, informē par to piederības dalībvalsts kompetento iestādi un nodrošina, ka tiek izpildīti šādi nosacījumi:

a. ar oficiālu līgumu vai attiecīgajā gadījumā esošas grupas iekšējo vienošanos, kas attiecas uz deleģēto ziņošanu, starp maksājumu pakalpojumu sniedzēju un trešo personu nepārprotami ir noteikta visu personu pienākumu sadale. It īpaši tajā skaidri noteikts tas, ka, neraugoties uz ziņošanas pienākuma iespējamo deleģēšanu, ietekmētais maksājumu pakalpojumu sniedzējs ir pilnībā atbildīgs par MPD2

96. pantā noteikto prasību izpildi un par tās informācijas saturu, kas iesniegta piederības dalībvalsts kompetentajai iestādei;

b. deleģēšana atbilst prasībām attiecībā uz tādu svarīgu darbības funkciju uzticēšanu ārpakalpojumu sniedzējiem, kas noteiktas

   i. MPD2 19. panta 6. punktā attiecībā uz maksājumu iestādēm un elektroniskās naudas iestādēm un ir piemērojamas pēc nepieciešamo izmaiņu veikšanas (*mutatis mutandis*) saskaņā ar Direktīvas 2009/110/EK (EMD) 3. pantu, vai

   ii. Eiropas Banku uzraudzītāju komitejas (*CEBS*) pamatnostādnēs par ārpakalpojumiem saistībā ar kredītiestādēm;

c. informāciju piederības dalībvalsts kompetentajai iestādei iesniedz iepriekš un jebkurā gadījumā, ja piemērojams, ievērojot kompetentās iestādes noteiktos termiņus un procedūras;

d. tiek pienācīgi nodrošināta jutīgu datu konfidencialitāte un kompetentajai iestādei iesniegtās informācijas kvalitāte, konsekvence, integritāte un uzticamība.

3.2. Maksājumu pakalpojumu sniedzējiem, kas vēlas, lai ieceltā trešā persona izpilda ziņošanas pienākumus konsolidētā veidā (t. i., iesniedzot vienu ziņojumu, kas attiecas uz vairākiem maksājumu pakalpojumu sniedzējiem, kurus ietekmējis viens un tas pats būtiskais operacionālais vai drošības incidents), ir jāinformē piederības dalībvalsts kompetentā iestāde, norādot kontaktinformāciju, kas iekļaujama formas sadaļā "Ietekmētais MPS", un jāpārliecinās, ka ir izpildīti šādi nosacījumi:

a. šo nosacījumu iekļauj līgumā par deleģēto ziņošanu;

b. nosaka to, ka konsolidētā ziņošana ir atkarīga no tā, ka incidentu izraisa trešās personas sniegto pakalpojumu pārtraukums;

c. ierobežo konsolidēto ziņošanu līdz maksājumu pakalpojumu sniedzējiem, kas ir izveidoti vienā un tajā pašā dalībvalstī;

d. nodrošina, ka trešā persona novērtē incidenta būtiskumu attiecībā uz katru ietekmēto maksājumu pakalpojumu sniedzēju un ietver konsolidētajā ziņojumā tikai tos maksājumu pakalpojumu sniedzējus, attiecībā uz kuriem minētais incidents ir atzīts par būtisku. Turklāt nodrošina, ka šaubu gadījumā maksājumu pakalpojumu sniedzējs ir ietverts konsolidētajā ziņojumā, kamēr nav pierādījumu, ka tam nevajadzētu būt ietvertam;

e. nodrošina, ka tad, ja veidnē ir lauki, kuros nav iespējams sniegt kopīgu atbildi (piem., B 2, B 4 vai C 3 sadaļa, trešā persona vai nu i) aizpilda to individuāli par katru ietekmēto maksājumu pakalpojumu sniedzēju, papildus precizējot katra tā

maksājumu pakalpojumu sniedzēja identitāti, uz kuru informācija attiecas, vai ii) lieto intervālus laukos, kuros tas ir iespējams, attēlojot zemākās un augstākās vērtības, kas konstatētas vai aplēstas attiecībā uz dažādajiem maksājumu pakalpojumu sniedzējiem;

f. maksājumu pakalpojumu sniedzējiem ir jānodrošina, ka trešā persona tos vienmēr informē par būtisku informāciju attiecībā uz incidentu un par visu saziņu starp trešo personu un kompetento iestādi, kā arī par tās saturu, taču tikai tādā mērā, kā iespējams, nepārkāpjot konfidencialitāti saistībā ar informāciju, kas attiecas uz citiem maksājumu pakalpojumu sniedzējiem.

3.3. Maksājumu pakalpojumu sniedzēji ziņošanas pienākumus nedrīkst deleģēt, ja tie iepriekš nav informējuši piederības dalībvalsts kompetento iestādi vai pēc tam, kad ir saņemta informācija, ka vienošanās par ārpakalpojumiem neatbilst 3.1. pamatnostādnes b) punktā izvirzītajām prasībām.

3.4. Maksājumu pakalpojumu sniedzēji, kas vēlas atsaukt deleģētos ziņošanas pienākumus, par šo lēmumu informē piederības dalībvalsts kompetento iestādi, ievērojot minētās kompetentās iestādes noteiktos termiņus un procedūras. Maksājumu pakalpojumu sniedzējiem ir jāinformē piederības dalībvalsts kompetentā iestāde arī par būtiskām norisēm, kas ietekmē iecelto trešo personu un tās spēju pildīt ziņošanas pienākumus.

3.5. Maksājumu pakalpojumu sniedzējiem ir pilnībā jāievēro savi ziņošanas pienākumi bez iespējas vērsties pēc ārējas palīdzības, ja ieceltā trešā persona neinformē piederības dalībvalsts kompetento iestādi par būtisku operacionālo vai drošības incidentu saskaņā ar MPD2 96. pantu un šīm pamatnostādnēm. Turklāt maksājumu pakalpojumu sniedzējiem ir jānodrošina, ka nerodas situācija, kad par incidentu paziņo divreiz — gan minētais maksājumu pakalpojumu sniedzējs, gan trešā persona.

4. pamatnostādne. Operacionālā un drošības politika

4.1. Maksājumu pakalpojumu sniedzējiem ir jānodrošina, ka vispārējā operacionālā un drošības politika skaidri definē visus pienākumus saistībā ar ziņošanu par incidentiem saskaņā ar MPD2, kā arī ieviestos procesus, lai īstenotu šajās pamatnostādnēs definētās prasības.

5. Pamatnostādnes, kuru adresāts ir kompetentās iestādes un kas attiecas uz kritērijiem, kā novērtēt incidenta būtiskumu, un incidentu ziņojuma elementiem, kas jādara zināmi citām valsts iestādēm

5. pamatnostādne. Incidenta būtiskuma novērtējums

5.1. Piederības dalībvalsts kompetentajām iestādēm ir jānovērtē būtisku operacionālo vai drošības incidentu nozīmīgums attiecībā uz citām valsts iestādēm, balstoties uz pašu ekspertu slēdzieniem un izmantojot šādus kritērijus kā minētā incidenta nozīmīguma primārie rādītāji:

a. incidenta cēloņi ietilpst citas valsts iestādes normatīvo uzdevumu lokā (t. i., tās kompetences jomā);
b. incidenta sekām ir ietekme uz citas valsts iestādes mērķiem (piem., finanšu stabilitātes aizsardzību);
c. incidents ietekmē vai varētu ietekmēt maksājumu pakalpojumu lietotājus plašā mērogā;
d. incidents ir plaši atspoguļots vai, visticamāk, tiks plaši atspoguļots plašsaziņas līdzekļos.

5.2. Piederības dalībvalsts kompetentās iestādes šo novērtējumu veic pastāvīgi incidenta pastāvēšanas laikā, lai identificētu iespējamas pārmaiņas, kas var padarīt par nozīmīgu incidentu, kurš iepriekš netika par tādu uzskatīts.

6. pamatnostādne. Informācija, kas jādara zināma

6.1. Neietekmējot citas normatīvās prasības sniegt ar incidentu saistītu informāciju citām valsts iestādēm, kompetentajām iestādēm informācija par būtiskiem operacionālajiem vai drošības incidentiem ir jādara zināma valsts iestādēm, kas identificētas, piemērojot 5.1. pamatnostādni (t. i., "citas attiecīgās valsts iestādes"), vismaz sākotnējā ziņojuma saņemšanas laikā (vai arī tāda ziņojuma laikā, kas noteicis, ka informācija ir jādara zināma) un tad, kad tām ir paziņots, ka pakalpojumu darbība atkal norit ierastajā gaitā (t. i., pēc pēdējā starpposma ziņojuma saņemšanas).

6.2. Kompetentajām iestādēm ir jāiesniedz citām attiecīgajām valsts iestādēm informācija, kas nepieciešama, lai skaidri atspoguļotu notikušo un iespējamās sekas. Lai to paveiktu, tām ir

jāsniedz vismaz informācija, kuru maksājumu pakalpojumu sniedzējs sniedz šādos formas laukos (vai nu sākotnējā, vai starpposma ziņojumā):

- incidenta konstatēšanas datums un laiks;
- incidenta sākšanās datums un laiks;
- datums un laiks, kad incidents tika novērsts vai kad ir paredzams, ka tas tiks novērsts;
- īss incidenta apraksts (tostarp detalizētā apraksta nekonfidenciālās ziņas);
- īss apraksts par veiktajiem vai plānotajiem pasākumiem ar mērķi atgūties no incidenta;
- apraksts par to, kā incidents varētu ietekmēt citus MPS un/vai infrastruktūras;
- atspoguļošanas plašsaziņas līdzekļos (ja tāda bijusi) apraksts;
- incidenta cēlonis.

6.3. Kompetentajām iestādēm pēc nepieciešamības dati ir jāpadara anonīmi un jāizslēdz tāda informācija, uz kuru varētu attiekties konfidencialitātes vai intelektuālā īpašuma ierobežojumi, pirms jebkāda ar incidentu saistītā informācija tiek nodota citām attiecīgajām valsts iestādēm. Taču kompetentajām iestādēm ir attiecīgajām valsts iestādēm jādara zināms ziņojumu iesniegušā maksājumu pakalpojumu sniedzēja nosaukums un adrese, ja minētās valsts iestādes var garantēt, ka tiks saglabāta informācijas konfidencialitāte.

6.4. Kompetentajām iestādēm vienmēr ir jāsaglabā tās informācijas konfidencialitāte un integritāte, kuru uzglabā un kopīgo ar citām attiecīgajām valsts iestādēm, kā arī pienācīgi jāautentificējas attiecībā uz citām attiecīgajām valsts iestādēm. It īpaši kompetentajām iestādēm attiecībā uz visu informāciju, kuru tās saņem saskaņā ar šīm pamatnostādnēm, ir jāpiemēro dienesta noslēpuma pienākumi, kas noteikti MPD2, neietekmējot piemērojamos Savienības tiesību aktus un valstu prasības.

6. Pamatnostādnes, kuru adresāts ir kompetentās iestādes un kas attiecas uz kritērijiem, kā novērtēt incidentu ziņojumu atbilstošos elementus, kuri jādara zināmi EBI un ECB, un uz saziņas formātu un procedūrām

7. pamatnostādne. Informācija, kas jādara zināma

7.1. Kompetentajām iestādēm vienmēr ir jāiesniedz EBI un ECB visi ziņojumi, ko tās ir saņēmušas no maksājumu pakalpojumu sniedzējiem (vai to vārdā), kurus ir ietekmējis būtisks operacionālais vai drošības incidents (t. i., sākotnējie, starpposma un noslēguma ziņojumi).

8. pamatnostādne. Komunikācija

8.1. Kompetentajām iestādēm vienmēr ir jāsaglabā tās informācijas konfidencialitāte un integritāte, kuru uzglabā un kopīgo ar EBI un ECB, kā arī pienācīgi jāautentificējas attiecībā uz EBI un ECB. It īpaši kompetentajām iestādēm attiecībā uz visu informāciju, kuru tās saņem saskaņā ar šīm pamatnostādnēm, ir jāpiemēro dienesta noslēpuma pienākumi, kas noteikti MPD2, neietekmējot piemērojamos Savienības tiesību aktus un valstu prasības.

8.2. Lai novērstu kavējumus, nosūtot ar incidentiem saistīto informāciju EBI/ECB, un samazinātu darbības pārtraukuma riskus, kompetentajām iestādēm ir jāatbalsta attiecīgi komunikācijas veidi.

1. pielikums. Ziņošanas formas maksājumu pakalpojumu sniedzējiem

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 - additional 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**

NORĀDES PAR FORMU AIZPILDĪŠANU

Maksājumu pakalpojumu sniedzējiem (MPS) ir jāaizpilda atbilstošās formas sadaļas atkarībā no aktuālā ziņošanas posma: A sadaļa — sākotnējam ziņojumam, B sadaļa — starpposma ziņojumiem, bet C sadaļa — noslēguma ziņojumam. Visi lauki ir jāaizpilda obligāti, ja vien nav skaidri norādīts citādi.

Virsraksts

Sākotnējais ziņojums: tas ir pirmais paziņojums, ko MPS iesniedz piederības dalībvalsts kompetentajai iestādei.

Starpposma ziņojums: tas ir iepriekšējā (sākotnējā vai starpposma) ziņojuma atjauninājums par to pašu incidentu.

Pēdējais starpposma ziņojums: ar to informē piederības dalībvalsts kompetento iestādi, ka ir atjaunotas ierastās darbības un pakalpojumu darbība noris kā ierasts, tāpēc vairs netiks iesniegti starpposma ziņojumi.

Noslēguma ziņojums: pēdējais ziņojums, ko MPS sūta par minēto incidentu, jo i) ir veikta pirmcēloņu analīze un aplēses var aizvietot ar faktiskiem datiem vai ii) incidents vairs nav uzskatāms par būtisku.

Incidents pārklasificēts kā nebūtisks: incidents vairs neatbilst kritērijiem, lai tiktu atzīts par būtisku, un nav paredzams, ka tas atbildīs minētajiem kritērijiem, pirms tas tiks atrisināts. MPS ir jāpaskaidro šīs klasifikācijas pazemināšanas iemesli.

Ziņojuma datums un laiks: precīzs datums un laiks, kad ziņojums tiek iesniegts kompetentajai iestādei.

Incidenta identifikācijas numurs, ja piemērojams (starpposma un noslēguma ziņojumam): atsauces numurs, ko kompetentā iestāde piešķir sākotnējā ziņojuma laikā, lai attiecīgā gadījumā nepārprotami identificētu incidentu (t. i., ja kompetentā iestāde piešķir šādu atsauces numuru).

A — sākotnējais ziņojums

A 1 — vispārēji dati

Ziņojuma veids:

Individuāls: ziņojums attiecas uz vienu MPS.

Konsolidēts: ziņojums attiecas uz vairākiem MPS, izmantojot konsolidētās ziņošanas iespēju. Lauki "Ietekmētais MPS" jāatstāj neaizpildīti (izņemot lauku "Incidenta ietekmētā(-ās) valsts/valstis"), un ziņojumā ir jāietver MPS saraksts, aizpildot atbilstošo tabulu (Konsolidētais ziņojums — MPS saraksts).

Ietekmētais MPS: attiecas uz MPS, kuram radies incidents.

MPS nosaukums: tā MPS pilns nosaukums, kuram ir jāveic ziņošanas procedūra, kā norādīts atbilstošajā oficiālajā valsts MPS reģistrā.

MPS unikālais identifikācijas numurs, ja piemērojams: atbilstošais unikālais identifikācijas numurs, ko izmanto katrā dalībvalstī, lai identificētu MPS, un ko piešķir MPS, ja lauks "MPS atļaujas numurs" nav aizpildīts.

MPS atļaujas numurs: atļaujas numurs piederības dalībvalstī.

Grupas galvenā sabiedrība: sabiedrību grupu gadījumā, kā definēts Eiropas Parlamenta un Padomes 2015. gada 25. novembra Direktīvas (ES) 2015/2366 par maksājumu pakalpojumiem iekšējā tirgū, ar ko groza Direktīvas 2002/65/EK, 2009/110/EK un 2013/36/EK un Regulu (ES) Nr. 1093/2010 un atceļ Direktīvu 2007/64/EK, 4. panta 40) punktā, lūdzu, norādiet galvenās sabiedrības nosaukumu.

Piederības valsts: dalībvalsts, kurā atrodas MPS juridiskā adrese; vai, ja MPS saskaņā ar valsts tiesību aktiem nav juridiskās adreses, tad dalībvalsts, kurā atrodas MPS galvenais birojs.

Incidenta ietekmētā(-ās) valsts/valstis: valsts vai valstis, kur ir radusies incidenta ietekme (piem., ir ietekmētas vairākas MPS filiāles, kas atrodas dažādās valstīs). Tā var būt vai var nebūt tā pati valsts, kas ir piederības dalībvalsts.

Primārā kontaktpersona: ietekmētā MPS tās personas vārds un uzvārds, kas ir atbildīga par ziņošanu par incidentu, vai, ja ietekmētā MPS uzdevumā ziņošanu veic trešā persona, tad par incidenta pārvaldību/riska nodaļu vai tamlīdzīgu jomu atbildīgās personas vārds un uzvārds.

E-pasts: e-pasta adrese, uz kuru pēc vajadzības var nosūtīt pieprasījumus sniegt papildu skaidrojumus. Tā var būt vai nu personiskā, vai uzņēmuma e-pasta adrese.

Tālrunis: tālruņa numurs, uz kuru zvanīt, lai pēc vajadzības pieprasītu sniegt papildu skaidrojumus. Tas var būt vai nu personiskais, vai uzņēmuma tālruņa numurs.

Sekundārā kontaktpersona: tādas citas personas vārds un uzvārds, ar kuru kompetentā iestāde var sazināties, lai uzzinātu par incidentu, ja primārā kontaktpersona nav sasniedzama. Ja ietekmētā MPS uzdevumā ziņojumu iesniedz trešā persona, tādas citas personas vārds un uzvārds ietekmētajā MPS, kas pārstāv incidenta pārvaldības/riska nodaļu vai tamlīdzīgu jomu.

E-pasts: citas kontaktpersonas e-pasta adrese, uz kuru pēc vajadzības var nosūtīt pieprasījumus sniegt papildu skaidrojumus. Tā var būt vai nu personiskā, vai uzņēmuma e-pasta adrese.

Tālrunis: citas kontaktpersonas tālruņa numurs, uz kuru zvanīt, lai pēc vajadzības pieprasītu sniegt papildu skaidrojumus. Tas var būt vai nu personiskais, vai uzņēmuma tālruņa numurs.

Ziņošanas iestāde: šo sadaļu aizpilda, ja ietekmētā MPS uzdevumā ziņošanas pienākumus pilda trešā persona.

Ziņošanas iestādes nosaukums: tās iestādes pilns nosaukums, kas ziņo par incidentu, kā norādīts atbilstošajā oficiālajā valsts komercreģistrā.

Unikālais identifikācijas numurs, ja atbilstoši: atbilstošais unikālais identifikācijas numurs, ko izmanto valstī, kurā atrodas trešā persona, lai identificētu iestādi, kas ziņo par incidentu, un kuru piešķir ziņošanas iestāde, ja nav aizpildīts lauks “Atļaujas numurs”.

Atļaujas numurs, ja piemērojams: trešās personas atļaujas numurs atrašanās vietas valstī, ja piemērojams.

Primārā kontaktpersona: tās personas vārds un uzvārds, kas ir atbildīga par ziņošanu par incidentu.

E-pasts: e-pasta adrese, uz kuru pēc vajadzības var nosūtīt pieprasījumus sniegt papildu skaidrojumus. Tā var būt vai nu personiskā, vai uzņēmuma e-pasta adrese.

Tālrunis: tālruņa numurs, uz kuru zvanīt, lai pēc vajadzības pieprasītu sniegt papildu skaidrojumus. Tas var būt vai nu personiskais, vai uzņēmuma tālruņa numurs.

Sekundārā kontaktpersona: tādas citas personas vārds un uzvārds iestādē, kas ziņo par incidentu, ar kuru kompetentā iestāde var sazināties, ja primārā kontaktpersona nav sasniedzama.

E-pasts: citas kontaktpersonas e-pasta adrese, uz kuru pēc vajadzības var nosūtīt pieprasījumus sniegt papildu skaidrojumus. Tā var būt vai nu personiskā, vai uzņēmuma e-pasta adrese.

Tālrunis: citas kontaktpersonas tālruņa numurs, uz kuru zvanīt, lai pēc vajadzības pieprasītu sniegt papildu skaidrojumus. Tas var būt vai nu personiskais, vai uzņēmuma tālruņa numurs.

A 2 — incidenta konstatēšana un sākotnējā klasifikācija

Incidenta konstatēšanas datums un laiks: datums un laiks, kad incidents pirmoreiz tika konstatēts.
Incidentu konstatēja: jānorāda, vai incidentu konstatēja maksājumu pakalpojumu lietotājs, cita persona MPS ietvaros (piem., veicot iekšējās revīzijas funkciju) vai ārēja persona (piem., ārējs pakalpojumu sniedzējs). Ja tas nebija neviens no uzskaitītajiem, lūdzu, atbilstošajā laukā sniedziet paskaidrojumu.
Īss, vispārīgs incidenta apraksts: lūdzu, īsi aprakstiet būtiskākās incidenta problēmas, norādot iespējamos cēloņus, tūlītējo ietekmi utt.
Kad ir paredzēts nākamais atjauninājums?: norādiet nākamā atjauninājuma (starpposma vai noslēguma ziņojuma) paredzēto iesniegšanas datumu un laiku.

B — starpposma ziņojums

B 1 — vispārēji dati

Detalizētāks incidenta apraksts: lūdzu, aprakstiet incidenta galvenās iezīmes, ietverot vismaz aptaujā iekļautos punktus (kāda ir konkrētā problēma, ar ko sastopas MPS, kā tā sākās un turpinājās, iespējamā saikne ar iepriekšēju incidentu, sekas, it īpaši attiecībā uz maksājumu pakalpojumu lietotājiem utt.).

Incidenta sākuma datums un laiks: datums un laiks, kad incidents sākās, ja zināms.

Incidenta statuss:

Diagnostika: incidenta iezīmes ir tikko identificētas.
Labošana: uzbrukuma skartie objekti tiek pārkonfigurēti.
Atgūšana: objekti, kuriem radusies kļūme, tiek atjaunoti pēdējā atgūstamajā stāvoklī.
Atjaunošana: atkal tiek nodrošināts ar maksājumu saistītais pakalpojums.

Datums un laiks, kad incidents tika novērsts vai kad ir paredzams, ka tas tiks novērsts: norādiet datumu un laiku, kad incidents tika novērsts vai kad ir paredzams, ka tas tiks kontrolēts, un kad pakalpojumu darbība noritēja vai kad ir paredzēts, ka tā noritēs, kā ierasts.

B 2 — incidenta klasifikācija / informācija par incidentu

Kopējā ietekme: lūdzu, norādiet, kuras dimensijas incidents ir ietekmējis. Var atzīmēt vairākus lodziņus.

Integritāte: īpašība, kas nozīmē, ka tiek garantēta aktīvu (arī datu) precizitāte un pilnīgums.
Pieejamība: īpašība, kas nozīmē, ka ar maksājumiem saistītie pakalpojumi ir pieejami maksājumu pakalpojumu lietotājiem un viņi var tos izmantot.
Konfidencialitāte: īpašība, kas nozīmē, ka informācija nav pieejama vai nav izpaužama personām, organizācijām vai procesiem, kuriem nav atbilstoša pilnvarojuma.
Autentiskums: īpašība, kas nozīmē, ka izcelsme atbilst apgalvotajam.
Nepārtrauktība: īpašība, kas nozīmē, ka organizācijas procesi, uzdevumi un aktīvi, kas nepieciešami, lai nodrošinātu ar maksājumu saistītus pakalpojumus, ir pilnībā pieejami un darbojas pieņemamos, iepriekš noteiktos līmeņos.

Ietekmētie darījumi: MPS ir jānorāda, kuras robežvērtības, ja tādas ir, incidents sasniedz vai, visticamāk, sasniegs, kā arī saistītie rādītāji — ietekmēto darījumu skaits, ietekmētie darījumi procentuāli no kopējā to maksājumu darījumu skaita, kas veikti, izmantojot tos pašus maksājumu pakalpojumus, kurus incidents ir ietekmējis, kā arī kopējā darījumu vērtība. MPS ir jāsniedz konkrētas šo mainīgo vērtības, kas var būt gan faktiskie skaitļi, gan aplēses. Iestādes, kas ziņo vairāku MPS uzdevumā (t. i., konsolidētā ziņošana), var norādīt vērtību intervālus, norādot zemākās un augstākās novērotās vai aplēstās vērtības ziņojumā ietverto MPS grupā, atdalot tās ar defisi. Parasti MPS jēdziens "ietekmētie darījumi" ir jāizprot kā visi pašmāju un pārrobežu darījumi,

kurus incidents ir tieši vai netieši ietekmējis vai, visticamāk, ietekmēs, jo īpaši tie darījumi, kurus nav bijis iespējams uzsākt vai apstrādāt, kuriem tika izmainīts maksājuma ziņojuma saturs un kuri tika pasūtīti krāpnieciski (neatkarīgi no tā, vai līdzekļi ir atgūti vai nav). Turklāt MPS jēdziens "maksājumu darījumu ierastais līmenis" ir jāizprot kā to ikdienas pašmāju un pārrobežu maksājumu darījumu vidējais skaits gadā, kurus veic, izmantojot tos pašus maksājumu pakalpojumus, kurus ietekmēja incidents, par atsauces periodu aprēķiniem ņemot iepriekšējo gadu. Ja MPS neuzskata, ka šis rādītājs ir reprezentatīvs (piem., sezonalitātes dēļ), viņiem tā vietā ir jāizmanto cits, reprezentatīvāks rādītājs un laukā "Komentāri" ir jāsniedz kompetentajai iestādei šādas pieejas pamatojums.

Ietekmētie maksājumu pakalpojumu lietotāji: MPS ir jānorāda robežvērtības, ja tādas ir, kuras incidentā ir sasniegtas vai, visticamāk, tiks sasniegtas, kā arī saistītie rādītāji — kopējais ietekmēto maksājumu pakalpojumu lietotāju skaits un ietekmēto maksājumu pakalpojumu lietotāju skaits procentuāli no kopējā maksājumu pakalpojumu lietotāju skaita. MPS ir jāsniedz konkrētas šo mainīgo vērtības, kas var būt gan faktiskie skaitļi, gan aplēses. Iestādes, kas ziņo vairāku MPS uzdevumā (t. i., konsolidētā ziņošana), var norādīt vērtību intervālus, norādot zemākās un augstākās novērotās vai aplēstās vērtības ziņojumā ietverto MPS grupā, atdalot tās ar defisi. MPS ir jāizprot jēdziens "ietekmētie maksājumu pakalpojumu lietotāji" kā visi klienti (pašmāju un ārzemju, patērētāji un uzņēmumi), kuriem ar ietekmēto maksājumu pakalpojumu sniedzēju ir noslēgts līgums, kas tiem piešķir piekļuvi ietekmētajam maksājumu pakalpojumam, un kuri ir cietuši vai, visticamāk, cietīs no incidenta sekām. MPS aplēses ir jābalsta uz iepriekšējām norisēm, lai noteiktu to maksājumu pakalpojumu lietotāju skaitu, kuri, iespējams, incidenta pastāvēšanas laikā ir izmantojuši minēto maksājumu pakalpojumu. Grupu gadījumā katram MPS ir jāņem vērā tikai paša maksājumu pakalpojumu lietotāji. Ja MPS piedāvā darbības pakalpojumus citiem, šim MPS ir jāņem vērā tikai savi maksājumu pakalpojumu lietotāji (ja tādi ir) un tiem MPS, kuri saņem šos darbības pakalpojumus, ir jānovērtē incidents saistībā ar saviem maksājumu pakalpojumu lietotājiem. Turklāt MPS kā kopējais maksājumu pakalpojumu lietotāju skaits ir jāpieņem to pašmāju un pārrobežu maksājumu pakalpojumu lietotāju kopskaits, ar kuriem incidenta laikā ir bijušas noslēgtas līgumattiecības (vai arī visnesenākais pieejamais rādītājs) un kuriem ir pieeja ietekmētajam maksājumu pakalpojumam neatkarīgi no to lieluma un no tā, vai tie ir uzskatāmi par aktīviem vai pasīviem maksājumu pakalpojumu lietotājiem.

Pakalpojuma dīkstāve: MPS ir jānorāda, vai incidentā ir sasniegta vai, visticamāk, tiks sasniegta robežvērtība, kā arī saistītais rādītājs — kopējais pakalpojuma dīkstāve. MPS ir jāsniedz konkrētas šā mainīgā vērtības, kas var būt gan faktiskie skaitļi, gan aplēses. Iestādes, kas ziņo vairāku MPS uzdevumā (t. i., konsolidētā ziņošana), var norādīt vērtību intervālu, norādot zemākās un augstākās novērotās vai aplēstās vērtības ziņojumā ietverto MPS grupā, atdalot tās ar defisi. MPS ir jāņem vērā laikposms, kurā jebkurš uzdevums, process vai kanāls, kas ir saistīts ar maksājumu pakalpojumu sniegšanu, nav vai, visticamāk, nebūs pieejams, tādējādi liedzot i) uzsākt un/vai veikt maksājumu pakalpojumu un/vai ii) piekļūt maksājumu kontam. MPS pakalpojuma dīkstāve ir jāaprēķina no brīža, kad dīkstāve sākas, un viņiem ir jāņem vērā gan laikposmi, kuros tie ir atvērti pakalpojumu darbībai, kas nepieciešama maksājumu pakalpojumu izpildei, gan arī laikposmi ārpus darba laika un uzturēšanas laikposmi, ja tas ir atbilstoši un piemērojami. Ja maksājumu pakalpojumu sniedzēji nevar noteikt, kad pakalpojuma dīkstāve ir sācies, viņiem izņēmuma kārtā pakalpojuma dīkstāve ir jāaprēķina no brīža, kad tas tika konstatēts.

Ekonomiskā ietekme: MPS ir jānorāda, vai incidentā ir sasniegta vai, visticamāk, tiks sasniegta robežvērtība, kā arī saistītie rādītāji — tiešās izmaksas un netiešās izmaksas. MPS ir jāsniedz konkrētas šo mainīgo vērtības, kas var būt gan faktiskie skaitļi, gan aplēses. Iestādes, kas ziņo vairāku MPS uzdevumā (t. i., konsolidētā ziņošana), var norādīt vērtību intervālu, norādot zemākās un augstākās novērotās vai aplēstās vērtības ziņojumā ietverto MPS grupā, atdalot tās ar

defisi. MPS ir jāņem vērā izmaksas, kas var būt gan tieši, gan netieši saistītas ar incidentu. Cita starpā MPS ir jāņem vērā ekspropriētie līdzekļi vai aktīvi, aparatūras vai programmatūras aizstāšanas izmaksas, citas tiesu vai atlīdzināšanas izmaksas, maksas, kas piemērotas līgumsaistību neizpildes dēļ, sankcijas, ārējas saistības un zaudētie ieņēmumi. Attiecībā uz netiešajām izmaksām MPS ir jāņem vērā tikai tās izmaksas, kas jau ir zināmas vai, visticamāk, radīsies.

Tiešās izmaksas: incidenta tiešo izmaksu naudas summa (EUR), tostarp līdzekļi, kas nepieciešami incidenta novēršanai (piem., ekspropriēti līdzekļi vai aktīvi, aparatūras un programmatūras nomaiņas izmaksas, izdevumi attiecībā uz līgumsaistību neizpildi).

Netiešās izmaksas: incidenta netiešo izmaksu summa (EUR) (piem., klientu tiesiskā aizsardzība / kompensācijas izmaksas, neizmantotu pakalpojumu darbības iespēju rezultātā zaudēti ieņēmumi).

Augsts iekšējās eskalācijas līmenis: MPS ir jāizvērtē, vai par incidentu tādēļ, kā tas ietekmē ar maksājumiem saistītus pakalpojumus, (visticamāk) tiks informēts informācijas direktors (vai līdzīga līmeņa amatpersona) ārpus periodiskās ziņošanas procedūras un nepārtraukti incidenta pastāvēšanas laikā. Deleģētās ziņošanas gadījumā eskalācija notiek trešās personas ietvaros. Tāpat MPS ir jāapsver, vai incidents ietekmē ar maksājumiem saistītus pakalpojumus tā, ka tā rezultātā ir noteikts vai, visticamāk, tiks noteikts krīzes režīms.

Citi potenciāli ietekmēti MPS vai attiecīgās infrastruktūras: maksājumu pakalpojumu sniedzējiem ir jānovērtē incidenta ietekme uz finanšu tirgu, ar ko saprot finanšu tirgus infrastruktūras un/vai karšu maksājumu shēmas, kuras atbalsta tos un citus MPS. It īpaši MPS ir jānovērtē, vai incidents (visticamāk) tiks replicēts citiem MPS neatkarīgi no tā, vai tas ir ietekmējis vai, visticamāk, ietekmēs finanšu tirgus infrastruktūru nevainojamu funkcionēšanu un vai tas ir negatīvi ietekmējis vai, visticamāk, negatīvi ietekmēs finanšu sistēmas stabilu darbību kopumā. MPS ir jāņem vērā dažādas dimensijas, piemēram, vai ietekmētais komponents/programmatūra ir patentēti vai vispārpieejami, vai negatīvi ietekmētais tīkls ir iekšējs vai ārējs un vai MPS ir pārtraucis vai, visticamāk, pārtrauks pildīt savus pienākumus tajās finanšu tirgus infrastruktūrās, kurās tas ir dalībnieks.

Ietekme uz reputāciju: MPS ir jāņem vērā atpazīstamības līmenis, kuru (pēc to rīcībā esošās informācijas) incidents ir panācis vai, visticamāk, panāks tirgū. It īpaši MPS ir jāņem vērā varbūtība, ka incidents izraisīs kaitējumu sabiedrībai kā piemērots rādītājs tā potenciālam ietekmēt viņu reputāciju. MPS ir jāņem vērā, vai i) incidents ir ietekmējis redzamu procesu un tāpēc, visticamāk, tiks apskatīts vai jau ir apskatīts plašsaziņas līdzekļos (ņemot vērā ne tikai tradicionālos plašsaziņas līdzekļus, piem., laikrakstus, bet arī emuārus, sociālos tīklus utt.), ii) nav ievērotas vai, visticamāk, netiks ievērotas normatīvās prasības, iii) sankcijas ir vai, visticamāk, tiks pārkāptas vai iv) iepriekš ir noticis tāda paša veida incidents.

B 3 — incidenta apraksts

Incidenta veids: norādiet, vai pēc jūsu ieskatiem tas ir operacionālais vai drošības incidents.

Operacionālais incidents: incidents, kas izriet no neatbilstošiem vai kļūdainiem procesiem, cilvēku un sistēmu kļūdām vai nepārvaramas varas apstākļiem, kuri ietekmē ar maksājumiem saistītu apstākļu integritāti, pieejamību, konfidencialitāti, autentiskumu un/vai nepārtrauktību.

Drošības incidents: neatļauta piekļuve MPS aktīviem, neatļauta to izmantošana, izpaušana, pārtraukšana, modificēšana vai iznīcināšana, kā rezultātā var būt ietekmēta ar maksājumiem saistītu pakalpojumu integritāte, pieejamība, konfidencialitāte, autentiskums un/vai nepārtrauktība. Tas var notikt, ja cita starpā pret MPS tiek veikti kiberuzbrukumi, ja drošības politiku dizains vai īstenošana nav adekvāti vai ja fiziskā drošība nav adekvāta.

Incidenta cēlonis: norādiet incidenta cēloni vai, ja tas vēl nav zināms, visticamāko cēloni. Var atzīmēt vairākus lodziņus.

Tiek izmeklēts: cēlonis vēl nav noskaidrots.

Ārējs uzbrukums: cēloņa avots ir ārējs, un tā mērķis ir MPS (piem., ļaunprogrammatūru uzbrukumi).

Iekšējs uzbrukums: cēloņa avots ir iekšējs, un tā mērķis ir MPS (piem., iekšējā krāpšana).

Uzbrukuma veids:

Izplatīšanas/pakalpojuma atteikuma (I/PA): mēģinājums padarīt tiešsaistes pakalpojumu nepieejamu, pārslogojot to ar datplūsmu no vairākiem avotiem.

Iekšējo sistēmu inficēšana: kaitnieciska darbība, kas uzbrūk datorsistēmām, cenšoties nozagt vietu cietajā diskā vai centrālā procesora (*CPU*) laiku, piekļūt privātai informācijai, sabojāt datus, sūtīt surogātpastu kontaktiem utt.

Mērķtiecīga uzlaušana: neatļauta izspiegošana, okšķerēšana un informācijas zagšana kibertelpā.

Cits: cita veida uzbrukums, no kura MPS ir cietis vai nu tieši, vai ar pakalpojumu sniedzēja starpniecību. It īpaši, ja ir bijis uzbrukums, kura mērķis ir autorizēšanās un autentificēšanās process, tad ir jāatzīmē šis lodziņš. Detalizētāka informācija jāpievieno brīvajā teksta laukā.

Ārēji notikumi: cēlonis ir saistīts ar notikumiem, kas galvenokārt ir ārpus organizācijas kontroles (piem., dabas katastrofas, tiesiskas problēmas, pakalpojumu darbības problēmas un atkarība no pakalpojumiem).

Cilvēka kļūda: incidentu izraisījusi cilvēka netīša kļūda, kas ir vai nu maksājumu procesa daļa (piem., augšupielādē nepareizo maksājumu pakešdatni maksājumu sistēmā), vai ir ar to kādā veidā saistīta (piem., nejauši ir atslēgta elektropadeve un maksājuma darbība ir apturēta).

Procesa kļūme: incidenta cēlonis ir neatbilstošs maksājuma procesa dizains vai izpilde, procesa kontroles un/vai atbalsta procesi (piem., maiņas/migrēšanas, pārbaudes, konfigurēšanas, veiktspējas, novērošanas process).

Sistēmas kļūme: incidenta cēlonis ir saistīts ar to sistēmu nepiemērotu dizainu, izpildi, komponentiem, specifikācijām, integrāciju vai komplicētību, kas atbalsta maksājuma darbību.

Cits: incidenta cēlonis, kas nav neviens no iepriekš uzskaitītajiem. Papildu dati jānorāda brīvajā teksta laukā.

Vai incidents jūs ietekmēja tieši vai netieši — ar pakalpojumu sniedzēja starpniecību?: incidenta mērķis var būt MPS tieši, vai arī tas var ietekmēt MPS netieši ar trešās personas starpniecību. Netiešas ietekmes gadījumā, lūdzu, norādiet pakalpojumu sniedzēja(-u) nosaukumu.

B 4 — incidenta ietekme

Ietekmētā(-ās) ēka(-as) (adrese), ja piemērojams: ja ir ietekmēta fiziska ēka, lūdzu, norādiet tās adresi.

Ietekmētie komerckanāli: norādiet kanālu vai kanālus, caur kuriem mijiedarbojas ar maksājumu pakalpojumu lietotājiem, kurus ir ietekmējis incidents. Var atzīmēt vairākus lodziņus.

Filiāles: pakalpojumu darbības vieta (kas nav galvenais birojs), kas ir MPS daļa bez juridiskas personas statusa un kas nepastarpināti veic dažus vai vairākus darījumus, kuri veido MPS pakalpojumu darbības neatņemamu sastāvdaļu. Visas pakalpojumu darbības

vietas, ko vienā dalībvalstī ir izveidojis MPS, kura mītne atrodas citā dalībvalstī, uzskata par vienu filiāli.

Bankas pakalpojumi tiešsaistē: datoru izmantošana, lai tiešsaistē veiktu finanšu darījumus.

Telefonbanka: telefonu izmantošana, lai veiktu finanšu darījumus.

Mobilā banka: īpašas bankas pakalpojumu lietotnes izmantošana viedtālrunī vai tamlīdzīgā ierīcē, lai veiktu finanšu darījumus.

Bankomāti: elektromehāniskas ierīces, kas ļauj maksājumu pakalpojumu lietotājiem izņemt skaidru naudu no saviem kontiem un/vai piekļūt citiem pakalpojumiem.

Pārdošanas punkts: komersanta fiziska telpa, kurā tiek sākts maksājuma darījums.

Cits: ietekmētais komercijas kanāls, kas nav neviens no iepriekš uzskaitītajiem. Papildu dati jānorāda brīvajā teksta laukā.

Ietekmētie maksājumu pakalpojumi: norādiet tos maksājumu pakalpojumus, kuri incidenta rezultātā nedarbojas atbilstoši. Var atzīmēt vairākus lodziņus.

Naudas ieskaitīšana maksājumu kontā: skaidras naudas nodošana MPS, lai to ieskaitītu maksājumu kontā.

Naudas izņemšana no maksājumu konta: pieprasījums, ko MPS saņem no sava maksājumu pakalpojumu lietotāja, izsniegt skaidru naudu un debitēt tā maksājumu kontu par atbilstošu summu.

Rīcībai ar maksājumu kontu nepieciešamās darbības: rīcības, kas jāveic maksājumu kontā, lai aktivizētu, deaktivizētu un/vai uzturētu to (piem., atvēršana, bloķēšana).

Maksājumu instrumentu iegūšana: maksājumu pakalpojums, kas ietver MPS vienošanos ar naudas saņēmēju par maksājumu darījumu akceptēšanu un apstrādāšanu, kā rezultātā naudas saņēmējam tiek pārskaitīti naudas līdzekļi.

Kredīta pārvedumi: maksājumu pakalpojums naudas saņēmēja maksājumu konta kreditēšanai, izmantojot maksājumu darījumu vai vairākus maksājuma darījumus no maksātāja maksājumu konta, ko atbilstoši maksātāja sniegtajām norādēm veic MPS, kurš ir maksātāja maksājumu konta turētājs.

Tiešie debeti: maksājumu pakalpojums maksātāja maksājuma konta debetēšanai, kurā maksājuma darījumu uzsāk maksājuma saņēmējs atbilstoši maksātāja piekrišanai, ko tas sniedzis saņēmējam, saņēmēja maksājumu pakalpojumu sniedzējam vai paša maksātāja maksājumu pakalpojumu sniedzējam.

Karšu maksājumi: maksājumu pakalpojums, kas ir balstīts uz maksājumu kartes shēmas infrastruktūras un pakalpojumu darbības noteikumiem, lai veiktu maksājuma darījumu, izmantojot jebkādu karšu, telekomunikāciju, digitālu vai IT ierīci vai programmatūru, ja tā rezultātā tiek veikts debetkartes vai kredītkartes darījums. Uz kartēm balstīti maksājumu darījumi neietver darījumus, kas balstīti uz cita veida maksājumu pakalpojumiem.

Maksājumu instrumentu izdošana: maksājumu pakalpojums, kas ietver MPS vienošanos ar maksātāju nodrošināt tam maksājumu instrumentu, ar kuru uzsākt un apstrādāt maksātāja maksājumu darījumus.

Naudas pārvedums: maksājumu pakalpojums, ar ko līdzekļus saņem no maksātāja, neizveidojot maksājuma kontus uz maksātāja vai saņēmēja vārda, un kura vienīgais mērķis ir pārskaitīt atbilstošu summu saņēmējam vai citam MPS, kas rīkojas saņēmēja vārdā, un/vai ar kuru šādus līdzekļus saņem saņēmēja vārdā un padara tos saņēmējam pieejamus.

Maksājuma sākšanas pakalpojumi: maksājumu pakalpojumi, ar ko uzsāk maksājuma rīkojumu pēc maksājumu pakalpojuma lietotāja pieprasījuma attiecībā uz maksājumu kontu, kura turētājs ir cits MPS.

Konta informācijas pakalpojumi: tiešsaistes maksājumu pakalpojumi, ar ko sniedz konsolidētu informāciju par vienu vai vairākiem maksājumu kontiem, kuru turētājs ir maksājumu pakalpojumu lietotājs vai nu citā MPS, vai vairākos MPS.

Cits: ietekmētais maksājumu pakalpojums, kas nav neviens no iepriekš uzskaitītajiem. Papildu dati jānorāda brīvajā teksta laukā.

Ietekmētās funkcionālās jomas: norādiet maksājumu procesa darbību vai darbības, kuras incidents ir ietekmējis. Var atzīmēt vairākus lodziņus.

Autentifikācija/autorizācija: procedūras, kas ļauj MPS pārbaudīt maksājumu pakalpojumu lietotāja identitāti vai konkrēta maksājumu instrumenta lietošanas derīgumu, tostarp lietotāja personalizēto drošības datu lietošanu un maksājumu pakalpojumu sniedzēja (vai trešās personas, kas rīkojas šā lietotāja vārdā) piekrišanu pārskaitīt līdzekļus vai vērtspapīrus.

Komunikācija: informācijas plūsma identificēšanas, autentifikācijas, paziņošanas un informēšanas nolūkā starp MPS, kas apkalpo kontu, un maksājuma sākšanas pakalpojumu sniedzējiem, konta informācijas pakalpojumu sniedzējiem, maksātājiem, saņēmējiem un citiem MPS.

Klīrings: pārskaitījumu rīkojumu pārskaitīšanas, salīdzināšanas un — atsevišķos gadījumos — apstiprināšanas process pirms norēķiniem, potenciāli ietverot rīkojumu ieskaitu un norēķina gala posteņu noteikšanu.

Tiešais norēķins: darījuma vai apstrādes pabeigšana ar mērķi dzēst dalībnieku pienākumus, pārskaitot līdzekļus, kad šo darbību veic pats ietekmētais MPS.

Netiešie norēķini: darījuma vai apstrādes pabeigšana ar mērķi dzēst dalībnieku pienākumus, pārskaitot līdzekļus, kad šo darbību veic cits MPS ietekmētā MPS vārdā.

Cits: ietekmētā funkcionālā joma, kas nav neviena no iepriekš uzskaitītajām. Papildu dati jānorāda brīvajā teksta laukā.

Ietekmētās sistēmas un komponenti: norādīt, kuru MPS tehnoloģiskās infrastruktūras daļu vai daļas ir ietekmējis incidents. Var atzīmēt vairākus lodziņus.

Lietotne/programmatūra: programmas, operētājsistēmas utt., kas atbalsta MPS nodrošināto maksājumu pakalpojumu sniegšanu.

Datubāze: datu struktūra, kas uzglabā personisku un maksājumu informāciju, kura nepieciešama, lai izpildītu maksājumu darbības.

Aparatūra: fiziskais tehnoloģiskais aprīkojums, kas darbina procesus un/vai uzglabā datus, kuri nepieciešami MPS, lai veiktu ar maksājumiem saistītās darbības.

Tīkls/infrastruktūra: publiski vai privāti telekomunikāciju tīkli, kas maksājumu procesa laikā ļauj apmainīties ar datiem un informāciju (piem., tīmeklis).

Cits: ietekmētā sistēma vai komponents, kas nav neviens no iepriekš uzskaitītajiem. Papildu dati jānorāda brīvajā teksta laukā.

Ietekmētais personāls: norādiet, vai incidents ir ietekmējis MPS personālu, un, ja tā, sniedziet detalizētākas ziņas brīvajā teksta laukā.

B 5 — incidenta seku mazināšana

Kādas darbības/pasākumi līdz šim ir veikti vai ir plānoti, lai atgūtos pēc incidenta?: lūdzu, norādiet datus par darbībām, kuras ir veiktas vai kuras ir plānots veikt, lai īstermiņā risinātu problēmas saistībā ar incidentu.

Vai ir aktivizēti pakalpojumu darbības nepārtrauktības plāni un/vai negadījuma seku novēršanas plāni?: lūdzu, norādiet, vai tie ir vai nav aktivizēti, un, ja ir, tad sniedziet visbūtiskākās ziņas par to, kas notika (t. i., kad plāni tika aktivizēti un kas tajos bija iekļauts).

Vai MPS incidenta dēļ ir atcēlis vai samazinājis kādas kontroles?: lūdzu, norādiet, vai MPS bija jāignorē atsevišķas kontroles (piem., jāpārstāj piemērot četru acu principu), lai atrisinātu problēmu saistībā ar incidentu, un, ja tā, sniedziet ziņas par pamatcēloņiem, kas pamato kontroļu samazināšanu vai atcelšanu.

C — noslēguma ziņojums

C 1 — vispārēji dati

Starpposma ziņojumā norādītās informācijas atjaunināšana (kopsavilkums): lūdzu, sniedziet papildinformāciju par veiktajām darbībām, lai atgūtos no incidenta un novērstu tā atkārtošanos, par pirmcēloņa analīzi, gūto pieredzi utt.

Incidenta slēgšanas datums un laiks: norādiet datumu un laiku, kad tika uzskatīts, ka incidents ir slēgts.

Vai ir atjaunotas sākotnējās kontroles?: ja incidenta dēļ MPS bija jāatceļ vai jāsamazina kontroles, norādiet, vai šādas kontroles ir atjaunotas, un sniedziet jebkādu papildinformāciju brīvajā teksta laukā.

C 2 — pirmcēloņu analīze un vēlākie pasākumi

Kāds bija pirmcēlonis, ja ir jau zināms?: lūdzu, paskaidrojiet, kāds ir incidenta pirmcēlonis vai, ja tas vēl nav zināms, pagaidu slēdzieni, kas gūti pirmcēloņa analīzes procesā. MPS var pievienot datni, kurā ir norādīta sīkāka informācija, ja uzskata, ka tas ir nepieciešams.

Galvenā veiktā vai plānotā koriģējošā rīcība/pasākumi, lai novērstu incidenta atkārtošanos, ja jau ir zināmi: lūdzu, aprakstiet galveno veikto vai plānoto rīcību, lai novērstu incidenta turpmāku atkārtošanos.

C 3 — papildinformācija

Vai informācija par incidentu ir darīta zināma citiem MPS informācijas nolūkos?: lūdzu, sniedziet pārskatu par MPS, ar kuriem ir veikta oficiāla vai neoficiāla saziņa, lai informētu par incidentu, norādot to MPS datus, kuri ir informēti, informāciju, kas tika darīta zināma, kā arī iemeslus šādas informācijas kopīgošanai.

Vai pret MPS ir vērstas tiesiskas darbības?: lūdzu, norādiet, vai noslēguma ziņojuma aizpildīšanas laikā MPS incidenta rezultātā ir cietusi no tiesiskām darbībām (piem., ir iesniegta prasība tiesā vai ir zaudēta licence).