

EBA/GL/2021/03

---

10. juuni 2021

---

## Muudetud suunised

---

olulistest intsidentidest direktiivi  
(EL) 2015/2366 kohaselt teatamise  
kohta

# 1. Järgimis- ja teatamiskohustus

---

## Käesolevate suuniste staatus

1. See dokument sisaldab suuniseid, mis on välja antud EBA määruse<sup>1</sup> artikli 16 kohaselt. Kooskõlas EBA määruse artikli 16 lõikega 3 peavad pädevad asutused ja finantseerimisasutused võtma mis tahes meetmeid, et suuniseid järgida.
2. Suunistes esitatakse Euroopa Pangandusjärelevalve (EBA) seisukoht nõuetekohase järelevalvetava kohta Euroopa Finantsjärelevalve Süsteemis ehk kuidas tuleks liidu õigust konkreetsetes valdkonnas kohaldada. EBA määruse artikli 4 punktis 2 määratletud pädevad asutused, kellele suuniseid kohaldatakse, peaksid neid järgima, kaasates need sobival viisil oma tavadesse (nt muutes oma õigusraamistikku või järelevalveprotsesse) ka siis, kui suunised on ette nähtud eelkõige finantseerimisasutustele.

## Teatamiskohustus

3. EBA määruse artikli 16 lõike 3 kohaselt peavad pädevad asutused teatama EBA-le (07.11.2021), kas nad järgivad või kavatsevad järgida käesolevaid suuniseid, või vastasel juhul mittejärgimise põhjused. Kui selleks tähtajaks teadet ei saada, peab EBA pädevat asutust nõudeid mitte täitvaks. Teated tuleks saata EBA veebilehel avaldatud vormil, märkides viite EBA/GL/2021/03. Teate peaksid saatma isikud, kes on asjakohaselt volitatud esitama oma pädeva asutuse nimel nõuete järgimise teateid. Nõuete järgimise staatuse mis tahes muutusest tuleb EBA-le teatada.
4. Kooskõlas EBA määruse artikli 16 lõikega 3 avaldatakse teated EBA veebilehel.

---

<sup>1</sup> Euroopa Parlamendi ja nõukogu 24. novembri 2010. aasta määrus (EL) nr 1093/2010, millega asutatakse Euroopa Järelevalveasutus (Euroopa Pangandusjärelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/78/EÜ (ELT L 331, 15.12.2010, lk 12).

## 2. Sisu, kohaldamisala ja mõisted

---

### Sisu

5. Käesolevad suunised põhinevad Euroopa Parlamendi ja nõukogu 25. novembri 2015. aasta direktiivi (EL) 2015/2366 (makseteenuste kohta siseturul, direktiivide 2002/65/EÜ, 2009/110/EÜ ning 2013/36/EL ja määruse (EL) nr 1093/2010 muutmise ning direktiivi 2007/64/EÜ kehtetuks tunnistamise kohta) artikli 96 lõikes 3 EBA-le antud volitustel.
6. Eelkõige täpsustatakse suunistes makseteenuse pakkujatele oluliste operatsiooniriski- või turvaintsidentide liigitamise kriteeriumid, samuti direktiivi (EL) 2015/2366 artikli 96 lõikes 1 sätestatud vorm ja menetlused, mida tuleb järgida intsidentidest päritoluliikmesriigi pädevale asutusele teatamisel.
7. Lisaks käsitletakse suunistes viise, kuidas need pädevad asutused peaksid hindama intsidendi asjakohasust ja intsidentiaruande üksikasju, mida nad peavad vastavalt direktiivi (EL) 2015/2366 artikli 96 lõikele 2 jagama riigi muude ametiasutustega.
8. Peale selle käsitletakse suunistes ka teatatud intsidentide asjakohaste üksikasjade jagamist Euroopa Pangandusjärelevalve (EBA) ja Euroopa Keskpangaga (EKP), et edendada ühist ja järjekindlat käsitlust.

### Kohaldamisala

9. Käesolevaid suuniseid kohaldatakse oluliste operatsiooniriski- ja turvaintsidentide liigitamise ja intsidentidest teatamisele vastavalt direktiivi (EL) 2015/2366 artiklile 96.
10. Suuniseid kohaldatakse kõigi „olulise operatsiooniriski- või turvaintsidentide“ määratluse alla kuuluvate intsidentide suhtes, hõlmates nii asutusesiseseid kui ka -väliseid intsidente, mis võivad olla kuritahtlikud või juhuslikud.
11. Suuniseid kohaldatakse ka siis, kui oluline operatsiooniriski- või turvaintsident toimub väljaspool liitu (nt kui intsident toimub väljaspool liitu asuvas ema- või tütarettevõttes) ning mõjutab liidus asuva makseteenuse pakkuja osutatavaid makseteenuseid kas otseselt (makseteenust osutab mõjutatud liiduväline ettevõtte) või kaudselt (makseteenuse pakkuja suutlikkus jätkata makseteenuste osutamist on intsidendi tulemusena muul viisil ohustatud).
12. Suuniseid kohaldatakse ka oluliste intsidentide suhtes, mis mõjutavad funktsioone, mida makseteenuste pakkujad on edasi andnud kolmandatele isikutele.

## Adressaadid

13. Suuniste esimene osa (4. jagu) on adresseeritud direktiivi (EL) 2015/2366 artikli 4 punktis 11 määratletud ja määruse (EL) 1093/2010 artikli 4 punktis 1 viidatud makseteenuse pakkujatele.
14. Suuniste teine ja kolmas osa (5. ja 6. jagu) on adresseeritud määruse (EL) 1093/2010 artikli 4 punkti 2 alapunktis i määratletud pädevatele asutustele.

## Mõisted

15. Kui ei ole sätestatud teisiti, on kõigil makseteenuste direktiivis kasutatud ja määratletud mõistetel siin suunistes sama tähendus. Peale selle kasutatakse suunistes järgmisi mõisteid:

Operatsiooniriski- või turvaintsident	Sündmus või mitu seotud sündmust, mida makseteenuse pakkuja ei ole kavandanud ja mis kahjustavad või tõenäoliselt kahjustavad maksetega seotud teenuste terviklust, käideldavust, konfidentsiaalsust ja/või autentsust.
Terviklus	Varade (sh andmete) täpsuse ja täielikkuse kaitsmine.
Käideldavus	Maksetega seotud teenuste täielik juurdepääsetavus ja kasutatavus makseteenuste kasutajatele vastavalt makseteenuste pakkuja poolt eelnevalt kindlaks määratud aktsepteeritavatele tasemetele.
Konfidentsiaalsus	Teavet ei tehta kättesaadavaks ega avalikustata volitamata isikutele, üksustele ega protsessidele.
Autentsus	Allikas on sama, mis see väidab end olevat.
Maksetega seotud teenused	Mis tahes äritegevus direktiivi (EL) 2015/2366 artikli 4 punkti 3 tähenduses ning kõik makseteenuste korrektseks osutamiseks vajalikud tehnilise toe toimingud.

## 3. Rakendamine

---

### Kohaldamise alguskuupäev

16. Suuniseid kohaldatakse alates 1. jaanuarist 2022.

### Kehtetuks tunnistamine

17. Alates 1. jaanuarist 2022 tunnistatakse kehtetuks järgmised suunised:

*Suunised olulistest intsidentidest direktiivi (EL) 2015/2366 kohaselt teatamise kohta  
(EBA/GL/2017/10)*

## 4. Suunised makseteenuse pakkujatele olulistest operatsiooniriski- ja turvaintsidentidest päritoluliikmesriigi pädevale asutusele teatamise kohta

---

### 1. suunis. Liigitamine oluliseks intsidendiks

1.1. Makseteenuse pakkujad peaksid liigitama oluliseks intsidendiks need operatsiooniriski- ja turvaintsendid, mis vastavad

- a. vähemalt ühele „kõrgema mõjutaseme“ kriteeriumile või
- b. vähemalt kolmele „madalama mõjutaseme“ kriteeriumile,

nagu on sätestatud suuniste punktis 1.4, järgides nendes suunistes kirjeldatud hindamist.

1.2. Makseteenuse pakkujad peaksid hindama operatsiooniriski- või turvaintsidenti järgmiste kriteeriumide ja seotud näitajate suhtes:

*i. Mõjutatud tehingud*

Makseteenuse pakkujad peaksid tegema kindlaks mõjutatud tehingute koguväärtuse ja kahjustatud maksete arvu protsendina mõjutatud makseteenuseid hõlmavate maksetehingute tavalasemest.

*ii. Mõjutatud makseteenuse kasutajad*

Makseteenuse pakkujad peaksid tegema kindlaks mõjutatud makseteenuse kasutajate absoluutarvu ja suhtarvu makseteenuse kasutajate koguarvu protsendina.

*iii. Võrgu või infosüsteemide turvalisuse rikkumine*

Makseteenuse pakkujad peaksid välja selgitama, kas kuritahtlik tegevus on ohustanud makseteenuste osutamise seotud võrgu või infosüsteemide turvalisust.

*iv. Teenuse seisuaeg*

Makseteenuse pakkujad peaksid tegema kindlaks ajavahemiku, mille vältel teenus ei ole makseteenuse kasutajale tõenäoliselt kättesaadav või mille vältel makseteenuse pakkuja ei saa täita maksekäsundit direktiivi (EL) 2015/2366 artikli 4 punkti 13 tähenduses.

*v. Majandusmõju*

Makseteenuse pakkujad peaksid tegema kindlaks intsidendiga seotud rahalised kulud tervikuna ning arvestama nende kulude absoluutsuurust ja (kui asjakohane) ka suhtelist olulisust seoses makseteenuse pakkuja suurusega (st seoses makseteenuse pakkuja esimese taseme omavahenditega).

*vi. Suur ettevõttesisene eskalatsioon*

Makseteenuse pakkujad peaksid välja selgitama, kas intsidendist on teavitatud või tõenäoliselt teavitatakse ettevõtte tippjuhtkonda.

*vii. Teised võimalikud mõjutatud makseteenuse pakkujad või asjakohased taristud*

Makseteenuse pakkujad peaksid tegema kindlaks intsidendiga tõenäoliselt kaasneva süsteemse mõju, st mõju võimaliku ülekandumise esialgu mõjutatud makseteenuse pakkujalt teistele makseteenuse pakkujatele, finantsturu taristutele ja/või makseskeemidele.

*viii. Mainemõju*

Makseteenuse pakkujad peaksid välja selgitama, kuidas võib intsident kahjustada kasutajate usaldust makseteenuse pakkuja vastu ja üldisemalt seotud teenuse või kogu turu vastu.

1.3. Makseteenuse pakkujad peaksid arvutama näitajate väärtuse vastavalt järgmisele meetodikale:

*i. Mõjutatud tehingud*

Üldiselt peaksid makseteenuse pakkujad mõistma „mõjutatud tehingutena“ kõiki riigisiseseid ja piiriüleseid tehinguid, mida intsident on mõjutanud või tõenäoliselt otseselt või kaudselt mõjutab, ning eriti tehinguid, mida ei õnnestunud algatada ega töödelda, mille makseteateise sisu muudeti ja mis telliti pettuse teel (olenemata sellest, kas vahendid on tagasi saadud või mitte) või mille nõuetekohane teostamine ei ole intsidendi tõttu muul moel võimalik või on takistatud.

Mis puudutab tehingute algatamise ja/või töötlemise võimalust mõjutavaid operatsiooniriskiintside, siis peaksid makseteenuse pakkujad teatama ainult sellistest intsidentidest, mis kestavad üle ühe tunni. Intsidendi kestust tuleks mõõta intsidendi toimumise hetkest kuni hetkeni, mil normaalne tegevus/operatsioonid taastati teenustasemele, millel neid enne intsidenti osutati.

Lisaks peaksid makseteenuse pakkujad mõistma maksetehingute tavatasemena aasta keskmist taset igapäevaste riigisiseste ja piiriüleste maksetehingute korral, mis tehti koos samade makseteenustega, mida intsident mõjutas, võttes arvutuste võrdlusperioodiks eelmise aasta. Kui makseteenuse pakkujad ei pea seda näitajat tüüpiliseks (nt hooajalisuse tõttu), tuleb kasutada muud iseloomulikumat mõõdikut ning esitada pädevale asutusele meetodi aluseks olevad põhjendused vormi vastaval väljal (vt lisa).

*ii. Mõjutatud makseteenuse kasutajad*

Makseteenuse pakkujad peaksid mõistma „mõjutatud makseteenuse kasutajatena“ kõiki kliente (riigisiseseid ja välisriikide kliente, tarbijaid ja juriidilisi isikuid), kellel on leping mõjutatud makseteenuse pakkujaga, kes tagab neile juurdepääsu mõjutatud makseteenusele, ning kes kannatasid või tõenäoliselt kannatavad intsidendi tagajärgede tõttu. Makseteenuse pakkujad peaksid varasema tegevuse põhjal hindama makseteenuse kasutajate arvu, kes võisid kasutada makseteenust intsidendi kestuse ajal.

Konsolideerimisgruppide puhul peaks iga makseteenuse pakkuja arvestama ainult enda makseteenuse kasutajaid. Kui makseteenuse pakkuja osutab teenuseid teistele makseteenuse pakkujatele, peaks ta arvestama ainult enda makseteenuse kasutajaid (kui need on olemas), ning neid teenuseid kasutavad makseteenuse pakkujad peaksid hindama intsidenti enda makseteenuse kasutajate suhtes.

Mis puudutab tehingute algatamise ja/või töötlemise võimalust mõjutavaid operatsiooniriskiintsidente, siis peaksid makseteenuse pakkujad teatama ainult sellistest intsidentidest, mis mõjutavad makseteenuse kasutajaid ja kestavad üle ühe tunni. Intsidenti kestust tuleks mõõta intsidenti toimumise hetkest kuni hetkeni, mil normaalne tegevus/operatsioonid taastati teenustasemele, millel neid enne intsidenti osutati.

Lisaks peaksid makseteenuse pakkujad käsutama makseteenuse kasutajate koguarvuna intsidenti toimumise ajal nendega lepingulises suhtes olnud selliste riigisiseste ja piiriüleste makseteenuse kasutajate koondarvu, kellel on juurdepääs mõjutatud makseteenusele, sõltumata nende suurusest või sellest, kas neid loetakse makseteenuse aktiivseteks või passiivseteks kasutajateks (või teise võimalusena kõige viimast kättesaadavat arvu).

#### *iii. Võrgu või infosüsteemide turvalisuse rikkumine*

Makseteenuse pakkujad peaksid välja selgitama, kas kuritahtlik tegevus on ohustanud makseteenuste osutamise seotud võrgu või infosüsteemide (sealhulgas andmete) käideldavust, autentsust, puutumatumust või konfidentsiaalsust.

#### *iv. Teenuse seisuaeg*

Makseteenuse pakkujad peaksid määrama kindlaks ajavahemiku, mil igasugune makseteenuse osutamisega seotud toiming, töötlemine või kanal on või on tõenäoliselt maas ning seega takistab i) makseteenuse algatamist ja/või täitmist ja/või ii) juurdepääsu maksekontole. Makseteenuse pakkujad peaksid arvestama teenuse seisuaega selle algushetkest, samuti tuleks arvestada nii ajavahemikke, mil nad on avatud äritegevuseks (nagu on vaja makseteenuste täitmiseks), kui ka ajavahemikke, mil nad on suletud, ning hooldusperioode, kui need on asjakohased ja kohaldatavad. Kui makseteenuse pakkujad ei suuda määrata kindlaks teenuse seisuaaja algust, peaksid nad erandkorras arvestama teenuse seisuaega alates selle avastamisest.

#### *v. Majandusmõju*

Makseteenuse pakkujad peaksid arvestama intsidendiga otseselt ja kaudselt seotud kulusid. Muu hulgas peaksid makseteenuse pakkujad arvestama sundvõõrandatud vahendeid või vara, riistvara või tarkvara asenduskulusid, muid kohtuekspertiiside või parandusmeetmete kulusid, lepingukohustuste mittetäitmise trahve, sanktsioone, väliseid kohustusi ja kaotatud tulu. Kaudsete kuludena peaksid makseteenuse pakkujad arvestama ainult kulusid, mis on juba teada või mille realiseerumine on väga tõenäoline.

#### *vi. Suur ettevõttesisene eskalatsioon*

Makseteenuse pakkujad peaksid kaalutlema, kas EBA IKT- ja turvariskide ohjamise suunistes määratletud juhtorganid on vastavalt EBA IKT- ja turvariskide ohjamise suuniste punkti 60



alpunktile d makseteenustele avaldunud mõju tõttu intsidendist teavitatud või teavitatakse tõenäoliselt väljaspool perioodilise teavitamise korda ja pidevalt terve intsidendi kestuse jooksul. Lisaks peaksid makseteenuse pakkujad kaalutlema, kas seoses intsidendi mõjuga makseteenustele käivitus või tõenäoliselt käivitub kriisiolukord.

vii. *Teised võimalikud mõjutatud makseteenuse pakkujad või asjakohased taristud*

Makseteenuse pakkujad peaksid hindama intsidendi mõju finantsturule, mida mõistetakse finantsturu taristutena ja/või makseskeemidena, mis toetavad neid ja teisi makseteenuse pakkujaid. Makseteenuse pakkujad peaksid eelkõige hindama, kas intsident kordus või tõenäoliselt kordub teiste makseteenuse pakkujatega, kas see on mõjutanud või tõenäoliselt mõjutab finantsturu taristute sujuvat toimimist ning kas see ohustas või tõenäoliselt ohustab finantssüsteemi kui terviku häireteta toimimist. Makseteenuse pakkujad peaksid meeles pidama eri mõõtmeid, näiteks kas mõjutatud komponent/tarkvara on ettevõttesisene või üldiselt kättesaadav, kas ohustatud võrk on ettevõttesisene või -väline ning kas makseteenuse pakkuja on katkestanud või tõenäoliselt katkestab oma kohustuste täitmise finantsturu taristutes, kuhu ta kuulub.

viii. *Mainemõju*

Makseteenuse pakkujad peaksid arvestama nähtavuse ulatust, mille intsident nende parima teadmise kohaselt turul saavutas või tõenäoliselt saavutab. Makseteenuse pakkujad peaksid eelkõige arvestama, et intsidendi poolt ühiskonnale tekitatava kahju tõenäosus näitab ilmekalt nende maine kahjustamise võimalikkust. Makseteenuse pakkujad peaksid arvestama, kas i) makseteenuse kasutajad ja/või teised makseteenuste osutajad on kaevanud intsidendi negatiivse mõju üle, ii) intsident on mõjutanud nähtavat makseteenusega seotud protsessi ja seda kajastatakse tõenäoliselt või on juba kajastatud meedias (peale tavapärase meedia, nt ajalehtede, ka blogides, suhtlusvõrgustikes jne), iii) lepingulised kohustused on jäetud täitmata või jäävad tõenäoliselt täitmata, mille tõttu algatatakse makseteenuse pakkuja vastu kohtuasju, iv) õigusaktidest tulenevad kohustused on jäetud täitmata, mille tõttu kohaldatakse järelevalvemeetmeid või sanktsioone, mille teave tehakse tõenäoliselt avalikkusele kättesaadavaks, ja v) sarnast tüüpi intsidente on ka varem esinenud.

- 1.4. Makseteenuse pakkujad peaksid intsidendi hindamisel tegema kindlaks iga üksikkriteeriumi korral, kas asjakohased tabeli 1 lüügid on saavutatud või saavutatakse tõenäoliselt enne intsidendi lahendamist.

Tabel 1. Lüügid

Kriteerium	Madalam mõjutase	Kõrgem mõjutase
Mõjutatud tehingud	> 10% makseteenuse pakkuja tehingute tavamäärast (tehingute arvu järgi) <b>ning</b> intsidendi kestus > 1 tund*	> 25% makseteenuse pakkuja tehingute tavamäärast (tehingute arvu järgi) <b>või</b>

	<b>või</b>  > 500 000 eurot <b>ning</b> intsidendi kestus > 1 tund*	> 15 000 000 eurot
Mõjutatud makseteenuse kasutajad	> 5000 <b>ning</b> intsidendi kestus > 1 tund*  <b>või</b>  > 10% makseteenuse pakkuja makseteenuse kasutajatest <b>ning</b> intsidendi kestus > 1 tund*	> 50 000  <b>või</b>  > 25% makseteenuse pakkuja makseteenuse kasutajatest
Teenuse seisuaeg	> 2 tundi	Ei kohaldata
Võrgu või infosüsteemide turvalisuse rikkumine	Jah	Ei kohaldata
Majandusmõju	Ei kohaldata	> Maksimaalselt (0,1% esimese taseme omavahenditest**, 200 000 eurot) <b>või</b> 5 000 000 eurot
Suur ettevõttesisene eskalatsioon	Jah	Jah ja tõenäoliselt kuulutatakse välja kriisiolukord (või samaväärne olukord)
Teised võimalikud mõjutatud makseteenuse pakkujad või asjakohased taristud	Jah	Ei kohaldata
Mainemõju	Jah	Ei kohaldata

\* Üle ühe tunni pikkuse intsidendi kestuse lävi kohaldub ainult operatsiooniriskiintsidentidele, mis mõjutavad makseteenuse pakkuja võimet tehinguid algatada ja/või töödelda.

\*\*Esimese taseme omavahendid on määratletud Euroopa Parlamendi ja nõukogu 26. juuni 2013. aasta määruse (EL) nr 575/2013 (krediitiasutuste ja investeerimisühingute suhtes kohaldatavate usaldatavusnõuete kohta ja määruse (EL) nr 648/2012 muutmise kohta) artiklis 25.

- 1.5. Makseteenuse pakkujad peaksid kasutama hinnangulisi andmeid, kui neil puuduvad tegelikud andmed, et hinnata, kas lävi on saavutatud või saavutatakse tõenäoliselt enne intsidendi lahendamist (nt võib see toimuda esialgse uurimise etapis).
- 1.6. Makseteenuse pakkujad peaksid intsidendi kestuse ajal seda pidevalt hindama, et tuvastada võimalikke intsidendi staatuse muutusi mitteolulisest oluliseks või olulisest mitteoluliseks. Igasugusest intsidendi staatuse olulisest mitteoluliseks muutumisest tuleb suunise 2.21 kohaselt kohe ja põhjendamatu viivitusega teavitada pädevat asutust.

## 2. suunis. Teavitamisprotsess

- 2.1. Makseteenuse pakkujad peaksid koguma kogu asjakohase teabe, koostama lisa vormi täitmise teel intsidendiaruande ning esitama selle päritoluliikmesriigi pädevale asutusele. Makseteenuse pakkujad peaksid täitma kõik vormi väljad vastavalt lisa juhiste.
- 2.2. Makseteenuse pakkujad peaksid ühe intsidendiga seotud esialgse, vahe- ja lõpparuande esitamiseks kasutama sama vormi. Makseteenuse pakkujad peaksid seega täitma vormi järkjärgult ja vajadusel eelnevates aruannetes esitatud teavet uuendama.
- 2.3. Samuti peaksid makseteenuse pakkujad viivitamata esitama päritoluliikmesriigi pädevale asutusele (kui asjakohane) koopia kasutajatele esitatud (või esitatavast) teabest, nagu on sätestatud direktiivi (EL) 2015/2366 artikli 96 lõikes 1.
- 2.4. Makseteenuse pakkujad peaksid oma päritoluliikmesriigi pädeva asutuse taotlusel esitama kõik standardvormi teavet täiendavad lisadokumendid. Makseteenuse pakkujad peaksid järelmeetmena vastama päritoluliikmesriigi pädevalt asutuselt saadud lisateabe või selgituste taotlustele varem esitatud dokumentide kohta.
- 2.5. Kooskõlas suunisega 2.1 peaksid makseteenuse pakkujad kogu pädevale asutusele esitatud dokumentides sisalduva täiendava teabe, mis esitati kas makseteenuse pakkuja algatusel või suunise 2.4 kohasel pädeva asutuse taotlusel, kajastama ka vormil.
- 2.6. Makseteenuse pakkujad peaksid alati hoidma päritoluliikmesriigi pädeva asutusega vahetatud teabe konfidentsiaalsust ja terviklust ning autentima end päritoluliikmesriigi pädevale asutusele nõuetekohaselt.

### Esiialgne aruanne

- 2.7. Makseteenuse pakkujad peaksid pärast operatsiooniriski- või turvaintsidenti oluliseks intsidendiks liigitamist esitama päritoluliikmesriigi pädevale asutusele esialgse aruande. Pädevad asutused peaksid esialgse aruande kättesaamist põhjendamatu viivitusega kinnitama ja määrama intsidendi üheseks tuvastamiseks unikaalse viitenumbri. Makseteenuse pakkujad peaksid uuendatud esialgse aruande või sama intsidendiga seotud vahe- ja lõpparuande esitamisel viitama sellele viitenumbrile, v.a juhul, kui vahe- ja lõpparuanne esitatakse koos esialgse aruandega.
- 2.8. Makseteenuse pakkujad peaksid nelja tunni jooksul pärast operatsiooniriski- või turvaintsidenti oluliseks intsidendiks liigitamist saatma pädevale asutusele esialgse aruande. Kui on teada, et pädeva asutuse teavituskanaalid ei ole sel ajal kättesaadavaid või ei toimi, peaksid makseteenuse pakkujad esialgse aruande saatma kohe, kui kanalid on jälle kättesaadavad/toimivad.
- 2.9. Makseteenuse pakkujad peaksid intsidendi liigitama vastavalt suunistele 1.1 ja 1.4 õigeaegselt pärast intsidendi tuvastamist, ent hiljemalt 24 tundi pärast intsidendi tuvastamist

ja põhjendamatu viivitusega pärast intsidendi liigitamiseks vajaliku teabe makseteenuse pakkujale kättesaadavaks saamist. Kui intsidendi liigitamiseks on vaja rohkem aega, peaksid makseteenuse pakkujad pädevale asutusele esitatud esialgses aruandes selle põhjuseid selgitama.

- 2.10. Makseteenuse pakkujad peaksid esitama esialgse aruande päritoluliikmesriigi pädevale asutusele ka siis, kui varasem mitteoluline operatsiooniriski- või turvaintsident muutub oluliseks. Sellisel juhul peaksid makseteenuse pakkujad saatma esialgse aruande pädevale asutusele kohe pärast intsidendi staatuse muutuse tuvastamist või – kui pädeva asutuse teavituskanalid ei ole sel ajal kättesaadavad või ei toimi – esitama aruande kohe, kui kanalid on jälle kättesaadavad/toimivad.
- 2.11. Makseteenuse pakkujad peaksid esialgsetes aruannetes esitama üldise teabe (st vormi A osa), märkides intsidendi põhitud ja eeldatavad tagajärjed, lähtudes intsidendi avastamise hetkel või oluliseks intsidendiks liigitamisel kättesaadavast teabest. Makseteenuse pakkujad peaksid kasutama hinnangulisi andmeid, kui tegelik teave ei ole kättesaadav.

## Vahearuanne

- 2.12. Makseteenuse pakkujad peaksid esitama vahearuande siis, kui normaalne tegevus on taastunud ja kõik toimib ettenähtud korras, teavitades sellest pädevat asutust. Makseteenuse pakkujad peaksid pidama tegevust jälle normaalseks siis, kui tegevus/tehingud on taastunud samale teenuste/tingimuste tasemele, nagu on määratlenud makseteenuse pakkuja või välises teenustaseme kokkuleppes (töötlemisajad, võimekus, turvanõuded jne), ning erandolukorra meetmed ei ole enam kasutusel. Vahearuanne peaks hõlmama intsidendi ja selle tagajärgede üksikasjalikumalt kirjeldust (vormi B osa).
- 2.13. Kui normaalne tegevus ei ole veel taastunud, peaksid makseteenuse pakkujad kolme tööpäeva jooksul pärast esialgset aruannet esitama pädevale asutusele vahearuande.
- 2.14. Makseteenuse pakkujad peaksid uuendama vormi A ja B osas varem esitatud teavet siis, kui nad on pärast eelmise teate esitamist saanud teada olulistest muutustest (nt kas intsident on eskaleerinud või on olukord rahunenud, kas on tuvastatud uusi põhjusi või on probleemi lahendamiseks võetud uusi meetmeid). See hõlmab olukorda, kus intsidenti ei ole kolme tööpäeva jooksul lahendatud, mistõttu makseteenuse pakkujatel tuleb esitada täiendav vahearuanne. Igal juhul peaksid makseteenuse pakkujad esitama täiendava vahearuande, kui päritoluliikmesriigi pädev asutus seda nõuab.
- 2.15. Sarnaselt esialgsete aruannetega peaksid makseteenuse pakkujad tegeliku teabe puudumisel kasutama hinnangulisi andmeid.
- 2.16. Kui normaalne tegevus taastub nelja tunni jooksul pärast intsidendi oluliseks liigitamist, peaksid makseteenuse pakkujad võtma eesmärgiks esitada korraga esialgse ja vahearuande (st täitma vormi A ja B osa) neljatunnise tähtaja jooksul.

## Lõpparuanne

- 2.17. Makseteenuse pakkujad peaksid esitama lõpparuande pärast juurpõhjuste analüüsimist (olenemata sellest, kas leevendusmeetmed on juba rakendatud või kas lõplik juurpõhjus on tuvastatud) ning võimalikud hinnangulised väärtused saab asendada tegelikega.
- 2.18. Makseteenuse pakkujad peaksid esitama lõpparuande pädevale asutusele kuni 20 tööpäeva jooksul pärast normaalse tegevuse taastumist. Kui makseteenuse pakkujad vajavad selle tähtaja pikendamist (nt kui mõju tegelikud arvanded ei ole veel kättesaadavad või kui juurpõhjused ei ole veel tuvastatud), peaksid nad enne tähtaja lõppu pöörduma pädeva asutuse poole, põhjendama viivitust ja pakkuma lõpparuande esitamise uue eeldatava kuupäeva.
- 2.19. Kui makseteenuse pakkujatel õnnestub esitada kogu lõpparuandes nõutav teave (st vormi C osa) 4 tunni jooksul pärast intsidendi oluliseks intsidendiks liigitamist, peaksid nad võtma eesmärgiks esitada esialgse, vahe- ja lõpparuande teave korraga.
- 2.20. Makseteenuse pakkujad peaksid esitama lõpparuandes täieliku teabe: i) hinnanguliste väärtuste asemel mõju tegelikud väärtused (samuti vormi A ja B osa muud vajalikud uuendused) ning ii) vormi C osa, milles on juurpõhjus, kui see on juba teada, ning probleemi kõrvaldamiseks ja selle edaspidiseks ennetamiseks rakendatud meetmete või kavandatavate meetmete kokkuvõtte.
- 2.21. Lisaks peaksid makseteenuse pakkujad saatma lõpparuande, kui intsidendi pideval hindamisel tuvastatakse, et juba teavitatud intsident ei vasta enam kriteeriumidele, mille alusel saaks selle liigitada oluliseks, ning eeldatavalt ei vasta intsident neile kriteeriumidele ka enne lahendamist. Sellisel juhul peaksid makseteenuse pakkujad saatma lõpparuande kohe, kui see olukord tuvastatakse, ning igal juhul järgmise aruande esitamise tähtjaks. Sellisel juhul peaksid makseteenuse pakkujad vormi C osa täitmise asemel tähistama märkeruudu „Intsident liigitub muuks kui oluliseks“ ning esitama intsidendi taseme ümberliigitamise põhjuste selgituse.

## 3. suunis. Delegeeritud ja konsolideeritud aruandlus

- 3.1. Pädeva asutuse loal võivad makseteenuse pakkujad, kes soovivad delegeerida direktiivi (EL) 2015/2366 kohaseid aruandluskohustusi kolmandale isikule, teatada sellest päritoluliikmesriigi pädevale asutusele ning täitma järgmised tingimused:
  - a. Vastutuse jagunemine kõigi poolte vahel määratletakse selgelt ametlikus lepingus või (kui kohaldatav) konsolideerimisgrupi sisekorras, mille alusel toimub makseteenuse pakkuja ja kolmanda isiku vaheline delegeeritud aruandlus. Eelkõige märgitakse selles, et sõltumata aruandluskohustuste võimalikust delegeerimisest on mõjutatud makseteenuse pakkuja täielikult vastutav ja aruandekohustuslik

direktiivi (EL) 2015/2366 artiklis 96 sätestatud nõuete täitmise ja päritoluliikmesriigi pädevale asutusele esitatava teabe sisu eest.

- b. Delegeerimine vastab oluliste tööülesannete edasiandmise nõuetele, nagu on sätestatud:
  - i. direktiivi (EL) 2015/2366 artikli 19 lõikes 6 seoses makseasutuste ja e-raha asutustega ja mida kohaldatakse *mutatis mutandis* vastavalt direktiivi 2009/110/EÜ artiklile 3, või
  - ii. EBA tegevuse edasiandmise suunistes (EBA/GL/2019/02) seoses kõigi makseteenuse pakkujatega.
- c. Teave esitatakse päritoluliikmesriigi pädevale asutusele varakult ja igal juhul järgides pädeva asutuse kehtestatud tähtaegu ja protseduure, kui see on kohaldatav.
- d. Pädevale asutusele esitatavate tundlike andmete konfidentsiaalsus ning teabe kvaliteet, sisu, terviklus ja usaldusväärsus on nõuetekohaselt tagatud.

3.2. Makseteenuse pakkujad, kes soovivad lubada määratud kolmandal isikul täita aruandluskohustust konsolideeritud viisil (esitama ühe aruande mitme makseteenuse pakkuja kohta, keda on mõjutanud sama oluline operatsiooniriski- või turvaintsident), peaksid teavitama päritoluliikmesriigi pädevat asutust, esitama kontaktandmed vormil „Mõjutatud makseteenuse pakkuja“ all ning tagama, et täidetud oleksid järgmised tingimused:

- a. see säte peab olema lisatud delegeeritud aruandluse aluslepingusse;
- b. konsolideeritud aruandluse eeltingimuseks on juhtum, mis on tingitud kolmanda isiku pakutavate teenuste häiretest;
- c. konsolideeritud aruandlus peab piirduma samas liikmesriigis tegutsevate makseteenuse pakkujatega;
- d. esitada tuleb kõigi intsidendist mõjutatud makseteenuse pakkujate nimekirj;
- e. tuleb tagada, et kolmas isik hindab intsidendi olulisust iga mõjutatud makseteenuse pakkuja jaoks ning lisab konsolideeritud aruandesse ainult need makseteenuse pakkujad, kelle jaoks intsident on liigitatud oluliseks; samuti tuleb tagada, et kahtluse korral on makseteenuse pakkuja konsolideeritud aruandesse lisatud, kui puuduvad vastupidist kinnitavad tõendid;
- f. kui vormil on välju, millel ei saa esitada ühist vastust (nt vormi punktid B 2, B 4 või C 3), peab kolmas isik i) täitma need iga makseteenuse pakkuja kohta eraldi,

märkides asjaomase makseteenuse pakkuja, või ii) kasutama kumulatiivseid väärtusi, mis tähistavad makseteenuse pakkujatel esinenud või hinnangulisi vähimaid ja suurimaid väärtusi;

- g. kolmas isik hoiab makseteenuse pakkujat pidevalt kursis kogu intsidendi olulise teabega ning võimaliku kolmanda isiku ja pädeva asutuse vahelise suhtluse ja selle sisuga, kuid ainult määral, mis välistaks teiste makseteenuse pakkujate teabe konfidentsiaalsuse võimaliku rikkumise.

- 3.3. Makseteenuse pakkujad ei tohiks delegerida oma aruandluskohustusi enne päritoluliikmesriigi pädeva asutuse teavitamist või pärast teate saamist, et tegevuse edasiandmise leping ei vasta suunise 3.1 punktis b viidatud nõuetele.
- 3.4. Kui makseteenuse pakkujad soovivad tühistada aruandluskohustuste delegerimise, tuleks see otsus teatada päritoluliikmesriigi pädevale asutusele vastavalt asutuse kehtestatud tähtaegadele ja protseduuridele. Samuti peaksid makseteenuse pakkujad teatama päritoluliikmesriigi pädevale asutusele kõik olulised arengud, mis mõjutavad määratud kolmandat isikut ja tema suutlikkust täita aruandluskohustusi.
- 3.5. Makseteenuse pakkujad peaksid täitma oma aruandluskohustusi piisavalt ilma välist abi kasutamata, kui kolmas isik ei teata päritoluliikmesriigi pädevale asutusele olulisest operatsiooniriski- ja turvaintsidentist vastavalt direktiivi (EL) 2015/2366 artiklile 96 ja käesolevatele suunistele. Makseteenuse pakkujad peaksid ka tagama, et intsidendi kohta ei esitataks aruannet kaks korda – makseteenuse pakkuja ise ja kolmas isik uuesti.
- 3.6. Makseteenuse pakkujad peaksid tagama, et kui intsident on tingitud tehnilise teenuse osutaja (või taristu) teenuste katkestusest, mis mõjutab mitut makseteenuse pakkujat, viidatakse delegeeritud aruandes konkreetse makseteenuse pakkuja individuaalsetele andmetele (v.a konsolideeritud aruande korral).

## 4. suunis. Operatsiooniriski- ja turvapoliitika

- 4.1. Makseteenuse pakkujad peaksid tagama, et nende üldises operatsiooniriski- ja turvapoliitikas oleks selgelt määratletud kogu direktiivi (EL) 2015/2366 kohane intsidentist teatamisega seotud vastutus, samuti käesolevates suunistes määratletud nõuete täitmiseks rakendatavad protsessid.

## 5. Suunised pädevatele asutustele intsidendi asjakohasuse hindamise kriteeriumide ja riigi muude ametiasutustega jagatavate intsidendiaruannete üksikasjade kohta

---

### 5. suunis. Intsidendi asjakohasuse hindamine

- 5.1. Päritoluliikmesriigi pädevad asutused peaksid hindama oluliste operatsiooniriski- ja turvaintsidentide asjakohasust riigi muude ametiasutuste jaoks, lähtudes iseenda eksperdiarvamusest ning kasutades intsidendi olulisuse põhinäitajana järgmisi kriteeriume:
- Intsidendi põhjused kuuluvad riigi muu ametiasutuse reguleerimispädevusse (st selle pädevusvaldkonda).
  - Intsidendi tagajärjed mõjutavad riigi muu ametiasutuse eesmärke (nt finantsstabiilsuse kaitset).
  - Intsident mõjutab või võib laialdaselt mõjutada makseteenuse pakkujaid.
  - Intsident saab tõenäoliselt või on saanud ulatuslikku meediakajastust.
- 5.2. Päritoluliikmesriigi pädevad asutused peaksid intsidendi kestuse ajal seda pidevalt hindama, et tuvastada muutused, mis võiksid muuta varem asjakohatuks peetud intsidendi asjakohaseks.

### 6. suunis. Jagatav teave

- 6.1. Olenemata muust õiguslikust alusest intsidendi teabe jagamiseks riigi muude ametiasutustega peaksid pädevad asutused esitama suunises 5.1 märgitud asjaomastele riigisisestele ametiasutustele oluliste operatsiooniriski- või turvaintsidentide teavet vähemalt esialgse aruande (või aruande, milles ajendati teavet jagama) kättesaamise ajal ning siis, kui neid teavitatakse normaalse tegevuse taastumisest (vahearuande esitamisel).
- 6.2. Pädevad asutused peaksid esitama riigi asjakohastele ametiasutustele teabe, mida on vaja juhtunust ja võimalikest tagajärgedest selge ülevaate saamiseks. Selleks peaksid nad esitama vähemalt makseteenuse pakkujalt saadud teabe järgmistel vormi väljadel (esialgses või vahearuandes):
- intsidendi oluliseks liigitamise kuupäev ja kellaaeg;
  - intsidendi avastamise kuupäev ja kellaaeg;
  - intsidendi alguse kuupäev ja kellaaeg;



- intsidendist taastumise või eeldatava taastumise kuupäev ja kellaaeg;
  - intsidendi lühikirjeldus (sh üksikasjaliku kirjelduse mittetundlikud osad);
  - intsidendist taastumiseks rakendatud või kavandatavate meetmete lühikirjeldus;
  - kirjeldus, kuidas võib intsident mõjutada teisi makseteenuse pakkujaid ja/või taristuid;
  - meediakajastuse kirjeldus (kui on olemas);
  - intsidendi põhjus.
- 6.3. Enne intsidendi teabe jagamist riigi asjakohaste ametiasutustega peaksid pädevad asutused vajaduse korral teabe nõuetekohaselt anonüümima ning jätma välja teabe, millele võivad kehtida konfidentsiaalsus- või intellektuaalomandipiirangud. Sellegipoolest peaksid pädevad asutused esitama riigi asjakohastele ametiasutustele aruande esitanud makseteenuse pakkuja nime ja aadressi, kui need riigi ametiasutused tagavad, et teavet töödeldakse konfidentsiaalselt.
- 6.4. Pädevad asutused peaksid alati säilitama salvestatud ja jagatud teabe konfidentsiaalsuse ja tervikluse ning autentima end nõuetekohaselt riigi muude asjakohaste ametiasutuste jaoks. Pädevad asutused peaksid eelkõige töötleva kogu käesolevate suuniste kohaselt saadud teavet kooskõlas direktiivis (EL) 2015/2366 sätestatud ametisaladuse hoidmise kohustusega, ilma et see piiraks kohaldatavat liidu õigust ja riiklikke nõudeid.

## 6. Suunised pädevatele asutustele EBA-ga ja EKP-ga jagatavate intsidendiaruannete üksikasjade asjakohasuse hindamise kriteeriumide ning sellise teabevahetuse vormi ja menetluste kohta

---

### 7. suunis. Jagatav teave

- 7.1. Pädevad asutused peaksid alati esitama EBA-le ja EKP-le kõik olulisest operatsiooniriski- või turvaintsidendist mõjutatud makseteenuse pakkujatelt (või nende nimel) saadud aruanded, kasutades EBA veebilehel avaldatud standardvormi.

### 8. suunis. Teabevahetus

- 8.1. Pädevad asutused peaksid alati säilitama salvestatud ning EBA-ga ja EKP-ga jagatud teabe konfidentsiaalsuse ja tervikluse ning autentima end nõuetekohaselt EBA-le ja EKP-le. Pädevad asutused peaksid eelkõige töötleva kogu käesolevate suuniste kohaselt saadud teavet kooskõlas direktiivis (EL) 2015/2366 sätestatud ametisaladuse hoidmise kohustusega, ilma et see piiraks kohaldatavat liidu õigust ja riiklikke nõudeid.
- 8.2. Viivituste vältimiseks intsidendiga seotud teabe edastamisel EBA-le/EKP-le ning tegevuse katkestustega seotud ohtude minimeerimiseks peaksid pädevad asutused toetama asjakohaseid teabevahetusvahendeid.

# 1. lisa. Aruandlusvormid makseteenuse pakkujatele

## Esiialgne aruanne

Esiialgne aruanne		4 tunni jooksul pärast intsidenti oluliseks liigitamist		Algsedista rippmenüüde valikud	
Aruande kuupäev (PPKK/AAAA)		Intsidenti viitenumber		Kellaeg (TTMM)	
<b>A. Esiialgne aruanne</b>					
<b>A 1. Üldandmed</b>					
<b>Aruande liik</b>					
Aruande liik					
<b>Mõjutatud makseteenuse pakkuja</b>					
Makseteenuse pakkuja nimi					
Makseteenuse pakkuja riiklik tunnusnumber					
Konsolideerimisgrupi juhtivateid, kui on olemas					
Intsidentist mõjutatud riik/riigid					
<input type="checkbox"/> AT <input type="checkbox"/> DE <input type="checkbox"/> FR <input type="checkbox"/> IT <input type="checkbox"/> LV <input type="checkbox"/> PT <input type="checkbox"/> BE <input type="checkbox"/> DK <input type="checkbox"/> LU <input type="checkbox"/> IS <input type="checkbox"/> MT <input type="checkbox"/> RO <input type="checkbox"/> BG <input type="checkbox"/> EE <input type="checkbox"/> GR <input type="checkbox"/> IR <input type="checkbox"/> NL <input type="checkbox"/> SE <input type="checkbox"/> CY <input type="checkbox"/> ES <input type="checkbox"/> HR <input type="checkbox"/> LT <input type="checkbox"/> NO <input type="checkbox"/> SI <input type="checkbox"/> CZ <input type="checkbox"/> FI <input type="checkbox"/> HU <input type="checkbox"/> LU <input type="checkbox"/> PL <input type="checkbox"/> SK					
Esimene kontaktisik				E-post	
Teine kontaktisik				E-post	
Esimene kontaktisik				Telefon	
Teine kontaktisik				Telefon	
<b>Aruandev üksus (täitke see osa, kui aruandev üksus ei ole delegeeritud aruande esitamise korral mõjutatud makseteenuse pakkuja)</b>					
Aruandva üksuse nimi					
Riiklik tunnusnumber					
Esimene kontaktisik				E-post	
Teine kontaktisik				E-post	
Esimene kontaktisik				Telefon	
Teine kontaktisik				Telefon	
<b>A 2. INTSIDENDI AVASTAMINE JA LIIGITAMINE</b>					
Intsidenti avastamise kuupäev ja kellaeg (PPKK/AAAA TT:MM)					
Intsidenti liigitamise kuupäev ja kellaeg (PPKK/AAAA TT:MM)					
Intsidenti avastaja					
Intsidenti kirjeldus					
Kriteeriumid, mille korral tuleb esitada olulise intsidenti aruanne					
<input type="checkbox"/> Mõjutatud tehingud <input type="checkbox"/> Mõjutatud makseteenuse kasutajad <input type="checkbox"/> Teenuse seisuaeg <input type="checkbox"/> Võrgu või infosüsteemi funktsionaalsuse rikkumine <input type="checkbox"/> Majandusmõju <input type="checkbox"/> Suur ettevõtteisene eskalatsioon <input type="checkbox"/> Teised võimalikud mõjutatud makseteenuse pakkujad võrreldavaid tegevusi <input type="checkbox"/> Mainemõju					
Intsidenti lühi- ja üldkirjeldus					
Mõju teistes ELi liikmesriikides, kui mõju avaldub					
Teiste asutuste teavitamine					
Esiialgse aruande hilinemisega esitamise põhjused				Kui „Jah“, täpsustage:	

## Vahearuanne

Olulise intsidenti aruanne	
Vahearuanne	maksimaalselt 3 tööpäeva jooksul pärast esialgse aruande esitamist
	<b>Algeadista rippmenüüde</b>
Aruande kuupäev (PPKKAAAA)	Kellaeg (TTMM)
Intsidenti viitenumber	
B. Vahearuanne	
B 1. ÜLDANDMED	
<b>Intsidenti üksikasjalikum kirjeldus:</b>	
Milles probleem seisneb?	
Kuidas intsident algas?	
Kuidas see arenes?	
Milised on tagajärjed (eelkõige makseteenuse kasutajatele)?	
Kas makseteenuse kasutajaid teavitati intsidentist?	<input type="checkbox"/> Kui „Jah”, täpsustage:
Kas see oli seotud varasema intsidenti / varasemate intsidentidega?	<input type="checkbox"/> Kui „Jah”, täpsustage:
Kas see mõjutas teisi teenuse osutajaid / kolmandaid isikuid või nad olid kaasatud?	<input type="checkbox"/> Kui „Jah”, täpsustage:
Kas alustati kriisihjega (ettevõttesiseses ja/või -välises)?	<input type="checkbox"/> Kui „Jah”, täpsustage:
Intsidenti alguse kuupäev ja kellaeg (kui need on juba teada) (PPKKAAAA TTMM)	
Intsidentist taastumise või eeldatava taastumise kuupäev ja kellaeg:	
Mõjutatud funktsionaalsed valdkonnad	<input type="checkbox"/> Autentimine/autoriseerimine <input type="checkbox"/> Otsearveldus <input type="checkbox"/> Teavevahetus <input type="checkbox"/> Kaudne arveldus <input type="checkbox"/> Kliring <input type="checkbox"/> Muu
Varasemates aruannetes tehtud muudatused	Kui „Muu”, täpsustage:
B 2. INTSIDENTI LIIGITAMINE / INTSIDENTI TEAVE	
Mõjutatud tehingud <sup>(2)</sup>	Mõjutatuse arv: <input type="text"/> Mõjutatud tehingute arv: <input type="text"/> Protsent tavapärasest tehingute arvust: <input type="text"/> Mõjutatud tehingute väärtus eurodes: <input type="text"/> Intsidenti kestus (kohaldu ainult operatsiooniriisintsidentide korral): <input type="text"/> Märkused: <input type="text"/>
Mõjutatud makseteenuse kasutajad <sup>(3)</sup>	Mõjutatuse arv: <input type="text"/> Mõjutatud makseteenuse kasutajate arv: <input type="text"/> Protsent kõigist makseteenuse kasutajatest: <input type="text"/>
Võrgu või infosüsteemi turvalisuse rikkumine	Kirjeldage mõju võrgule või infosüsteemidele
Teenuse seisuaeg	Teenuse kogu seisuaeg: Päevad: <input type="text"/> Tunnid: <input type="text"/> Minutid: <input type="text"/>
Majandusmõju	Mõjutatuse arv: <input type="text"/> Otsekulud eurodes: <input type="text"/> Kaudsed kulud eurodes: <input type="text"/>
Suur ettevõttesisene eskalatsioon	Kirjeldage intsidenti ettevõttesiseses eskalatsiooni taset, täpsustades, kas selle tõttu käivitati või käivitatakse tõenäoliselt kriisirežiim (või samaväärne reaktsioon). Kui käivitatakse, kirjeldage seda
Teised võimalikud mõjutatud makseteenuse pakkujad või asjakohased taristud	Kirjeldage, kuidas võib intsident mõjutada teisi makseteenuse pakkujaid ja/või taristuid
Mainemõju	Kirjeldage, kuidas võib intsident mõjutada makseteenuse pakkuja mainet (nt meediakajastus, kohtuasjade algatamine või rikkumismenetlused...)
B 3. INTSIDENTI KIRJELDUS	
Intsidenti kirjeldus	
Intsidenti põhjus	<input type="checkbox"/> Põhjust uuritakse <input type="checkbox"/> Kuritahtlik tegevus <input type="checkbox"/> Protsessi rike <input type="checkbox"/> Süsteemi rike <input type="checkbox"/> Inimlik eksimus <input type="checkbox"/> Valissündmused <input type="checkbox"/> Muu
Kas intsident mõjutas teid otseselt või kaudselt teenusepakkuja kaudu?	<input type="checkbox"/> Kui „Kaudselt”, täpsustage vastava teenusepakkuja nimi:
B 4. INTSIDENTI MÕJU	
Üldmõju	<input type="checkbox"/> Terviklik <input type="checkbox"/> Käideldav <input type="checkbox"/> Konfidentsiaalsus <input type="checkbox"/> Autentne
Mõjutatud kommertskanalid	<input type="checkbox"/> Filiaalid <input type="checkbox"/> E-pangandus <input type="checkbox"/> E-kaubandus <input type="checkbox"/> Telefonipangandus <input type="checkbox"/> Mobilipangandus <input type="checkbox"/> Müügikoht <input type="checkbox"/> Muu
Mõjutatud makseteenused	<input type="checkbox"/> Sularaha ülekanne maksekontole <input type="checkbox"/> Sularaha väljavõtt maksekontolt <input type="checkbox"/> Maksekonto teenindamiseks vajalikud toimingud <input type="checkbox"/> Makseinstrumentide taotlemine <input type="checkbox"/> Makseinstrumentide väljastamine <input type="checkbox"/> Krediidiorraldused <input type="checkbox"/> Otsekorraldused <input type="checkbox"/> Kaardimaksud <input type="checkbox"/> Rahasire <input type="checkbox"/> Makse algatamise <input type="checkbox"/> Kontoteabe teenused
B 5. INTSIDENTI MÕJU LEEVENDAMINE	
Mis meetmeid on seni rakendatud või kavatakse rakendada intsidentist taastumiseks?	
Kas talituspidevuse ja/või taasteplaani on käivitatud?	
Kui on, siis millal? (PPKKAAAA TTMM)	
Kui on, kirjeldage	

## Lõpparuanne

Olulise intsidendi aruanne																																														
Valige aruande liik: <input type="text"/>	20 toopäeva jooksul pärast vahearuande esitamist																																													
Kirjeldage: (kohaldub intsidentidele, mis on ümber liigitatud mitteoluliseks)	<input type="text"/>																																													
Aruande kuupäev (PPKK/AAAA)	Kellaeg (TT:MM)																																													
Intsidendi viitenumber	<input type="text"/>																																													
<b>Algsedista rippmentüide valikud</b>																																														
C. LÕPPARUANNE																																														
<i>Kui vahearuannet ei ole saadetud, täidke ka B osa</i>																																														
C 1. ÜLDANDMED																																														
<b>Eslalgses aruandes ja vahearuandes/vahearuannetes esitatud teabe uuendus</b>																																														
Varasemates aruannetes tehtud muudatused	<input type="text"/>																																													
Muu asjakohane teave	<input type="text"/>																																													
<b>Kas kõik algsed kontrollid on jälle kasutusel?</b>	<input type="text"/>																																													
Kui ei ole, täpsustage, millised algsed kontrollid ei ole veel kasutusel ja kui pikka perioodi on vaja nende taastamiseks																																														
C 2. JUURPÕHJUSE ANALÜÜS JA JÄRELTOIMINGUD																																														
Mis oli juurpõhjus (kui see on juba teada)?	<input type="checkbox"/> Kuritahtlik tegevus <input type="checkbox"/> Protsessirike <input type="checkbox"/> Süsteemirike <input type="checkbox"/> Inimlik eksimus <input type="checkbox"/> Välistõendus <input type="checkbox"/> Muu																																													
Täpsustage:	<table border="0"> <tr> <td><input type="checkbox"/> Ründeкод</td> <td><input type="checkbox"/> Ebapiisarjärelevake ja otse</td> <td><input type="checkbox"/> Põistvara rike</td> <td><input type="checkbox"/> Tundmatu</td> <td><input type="checkbox"/> Tarnija/tehnilise teenuse osutaja rike</td> </tr> <tr> <td><input type="checkbox"/> Teabe kogumine</td> <td><input type="checkbox"/> Teavitamisprobleemid</td> <td><input type="checkbox"/> Võlgurike</td> <td><input type="checkbox"/> Tegevusetus</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Sissetungid</td> <td><input type="checkbox"/> Ebaõige käitamine</td> <td><input type="checkbox"/> Andmebaasi</td> <td><input type="checkbox"/> Ebapiisarvad ressursid</td> <td><input type="checkbox"/> Vääraratumüübid</td> </tr> <tr> <td><input type="checkbox"/> Häjus-/ummitusarüüne (DDoS)</td> <td><input type="checkbox"/> Ebapiisar müüstatutejuhüimine</td> <td><input type="checkbox"/> Tarkvara/takenduse rike</td> <td><input type="checkbox"/> Muu</td> <td><input type="checkbox"/> Muu</td> </tr> <tr> <td><input type="checkbox"/> Tähtlik ettevõtte esine tegevus</td> <td><input type="checkbox"/> Ettevõtte teie kasutade ja dokumentide ebapiisar</td> <td><input type="checkbox"/> Füüsiline kahju</td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/> Tähtlik ettevõtte väliline füüsiline kahju</td> <td><input type="checkbox"/> Täasteprobleemid</td> <td><input type="checkbox"/> Muu</td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/> Teabesisu tute</td> <td><input type="checkbox"/> Muu</td> <td></td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/> Pettus</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/> Muu</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	<input type="checkbox"/> Ründeкод	<input type="checkbox"/> Ebapiisarjärelevake ja otse	<input type="checkbox"/> Põistvara rike	<input type="checkbox"/> Tundmatu	<input type="checkbox"/> Tarnija/tehnilise teenuse osutaja rike	<input type="checkbox"/> Teabe kogumine	<input type="checkbox"/> Teavitamisprobleemid	<input type="checkbox"/> Võlgurike	<input type="checkbox"/> Tegevusetus		<input type="checkbox"/> Sissetungid	<input type="checkbox"/> Ebaõige käitamine	<input type="checkbox"/> Andmebaasi	<input type="checkbox"/> Ebapiisarvad ressursid	<input type="checkbox"/> Vääraratumüübid	<input type="checkbox"/> Häjus-/ummitusarüüne (DDoS)	<input type="checkbox"/> Ebapiisar müüstatutejuhüimine	<input type="checkbox"/> Tarkvara/takenduse rike	<input type="checkbox"/> Muu	<input type="checkbox"/> Muu	<input type="checkbox"/> Tähtlik ettevõtte esine tegevus	<input type="checkbox"/> Ettevõtte teie kasutade ja dokumentide ebapiisar	<input type="checkbox"/> Füüsiline kahju			<input type="checkbox"/> Tähtlik ettevõtte väliline füüsiline kahju	<input type="checkbox"/> Täasteprobleemid	<input type="checkbox"/> Muu			<input type="checkbox"/> Teabesisu tute	<input type="checkbox"/> Muu				<input type="checkbox"/> Pettus					<input type="checkbox"/> Muu				
<input type="checkbox"/> Ründeкод	<input type="checkbox"/> Ebapiisarjärelevake ja otse	<input type="checkbox"/> Põistvara rike	<input type="checkbox"/> Tundmatu	<input type="checkbox"/> Tarnija/tehnilise teenuse osutaja rike																																										
<input type="checkbox"/> Teabe kogumine	<input type="checkbox"/> Teavitamisprobleemid	<input type="checkbox"/> Võlgurike	<input type="checkbox"/> Tegevusetus																																											
<input type="checkbox"/> Sissetungid	<input type="checkbox"/> Ebaõige käitamine	<input type="checkbox"/> Andmebaasi	<input type="checkbox"/> Ebapiisarvad ressursid	<input type="checkbox"/> Vääraratumüübid																																										
<input type="checkbox"/> Häjus-/ummitusarüüne (DDoS)	<input type="checkbox"/> Ebapiisar müüstatutejuhüimine	<input type="checkbox"/> Tarkvara/takenduse rike	<input type="checkbox"/> Muu	<input type="checkbox"/> Muu																																										
<input type="checkbox"/> Tähtlik ettevõtte esine tegevus	<input type="checkbox"/> Ettevõtte teie kasutade ja dokumentide ebapiisar	<input type="checkbox"/> Füüsiline kahju																																												
<input type="checkbox"/> Tähtlik ettevõtte väliline füüsiline kahju	<input type="checkbox"/> Täasteprobleemid	<input type="checkbox"/> Muu																																												
<input type="checkbox"/> Teabesisu tute	<input type="checkbox"/> Muu																																													
<input type="checkbox"/> Pettus																																														
<input type="checkbox"/> Muu																																														
Muu asjaomane teave juurpõhjuste kohta	<input type="text"/>																																													
Peamised rakendatud parandusmeetmed või kavandatavad meetmed intsidendi kordumise takistamiseks tulevikus, kui on juba teada	<input type="text"/>																																													
C 3. LISATEVAE																																														
Kas intsidendi teavet on jagatud teiste makseteenuse pakkujatega teavitamise eesmärgil?	Kui on, esitage täpsemad andmed: <input type="text"/>																																													
Kas makseteenuse pakkuja suhtes on rakendatud õiguslikke meetmeid?	Kui on, esitage täpsemad andmed: <input type="text"/>																																													
Võetud meetmete tulemuslikkuse hindamine	Esitage täpsemad andmed: <input type="text"/>																																													

## VORMIDE TÄITMISE JUHISED

Makseteenuse pakkujad peaksid täitma vormi asjaomase osa sõltuvalt aruandlusetaapist: esialgse aruande jaoks A osa, vahearuanne jaoks B osa ja lõpparuande jaoks C osa. Makseteenuse pakkujad peaksid sama intsidendi kohta esialgse, vahe- ja lõpparuande esitamisel kasutama sama vormi. Kõik väljad on kohustuslikud, kui ei ole selgesti märgitud teisiti.

### Pealkiri

**Esiagne aruanne:** esimene teade, mille makseteenuse pakkuja esitab päritoluliikmesriigi pädevale asutusele.

**Vahearuanne:** sisaldab intsidendi ja selle tagajärgede üksikasjalikumalt kirjeldust. See on sama intsidendi kohta esitatud esialgse aruande (ja vastavatel juhtudel eelneva vahearuande) uuendus.

**Lõpparuanne:** viimane aruanne, mille makseteenuse pakkuja saadab intsidendi kohta, sest i) juurpõhjuse analüüs on valmis ning hinnangulised väärtused saab asendada tegelikega või ii) intsidendi ei peeta enam oluliseks ja see tuleb ümber liigitada.

**Intsident liigitub muuks kui oluliseks:** intsident ei vasta enam kriteeriumidele, mille alusel saab seda pidada oluliseks, ning eeldatavalt ei hakka intsident vastama neile kriteeriumidele enne lahendamist. Makseteenuse pakkujad peaksid selgitama intsidendi ümberliigitamist.

**Aruande kuupäev ja kellaeg:** aruande pädevale asutusele esitamise täpne kuupäev ja kellaeg.

**Intsidendi viitenumber (kasutatakse vahe- ja lõpparuandes ning esialgse aruande uuendustes):** esialgse aruande esitamisel pädevalt asutuselt saadud intsidendi unikaalne viitenumber. Iga pädev asutus peaks eesliitena lisama vastava liikmesriigi kahenumbrilise ISO-koodi.

## A - Esialgne aruanne

### A 1 - Üldandmed

#### Aruande liik

**Individaalne:** aruanne hõlmab üht makseteenuse pakkujat.

**Konsolideeritud:** aruanne hõlmab mitut samas liikmesriigis tegutsevat makseteenuse pakkujat, keda mõjutab sama operatsiooniriski- või turvaintsident, mille tõttu konsolideeritud aruanne esitatakse. Jaotise „Mõjutatud makseteenuse pakkuja“ väljad tuleks jätta täitmata (v.a väli „Intsidentist mõjutatud riik/riigid“) ning aruandes sisalduvate makseteenuse pakkujate loetelu esitamiseks tuleb täita vastav tabel (konsolideeritud aruanne – makseteenuse pakkujate loetelu).

**Mõjutatud makseteenuse pakkuja:** makseteenuse pakkuja, kellel juhtus intsident.

**Makseteenuse pakkuja nimi:** aruandlusmenetluse alla kuuluva makseteenuse pakkuja täisnimi, nagu see on kantud kehtivasse ametlikku riiklikku makseteenuse pakkujate registrisse.

**Makseteenuse pakkuja riiklik tunnusnumber:** unikaalne riiklik tunnusnumber, mida päritoluliikmesriigi pädev asutus kasutab makseteenuse pakkuja üheselt tuvastamiseks oma riiklikus registris.

**Konsolideerimisgrupi juhtettevõtja:** direktiivi (EL) 2015/2366 artikli 4 lõikes 40 määratletud ettevõtjate grupi korral märkige juhtettevõtja nimi.

**Intsidentist mõjutatud riik/riigid:** riik või riigid, kus intsidendi mõju realiseerus (nt mõjutatud on ühe mitmes erinevas riigis asuva makseteenuse pakkuja mitu filiaali), sõltumata intsidendi raskusest teises riigis/riikides. Võib olla sama riik kui päritoluliikmesriik või mitte.

**Peamine kontaktisik:** intsidentist teatamise eest vastutava isiku ees- ja perekonnanimi, või kui mõjutatud makseteenuse pakkuja nimel teavitab kolmas teenuseosutaja, siis mõjutatud makseteenuse pakkuja intsidendi juhtimise eest vastutava / riskiosakonna või sarnase valdkonna eest vastutava isiku ees- ja perekonnanimi.

**E-post:** e-posti aadress, millelt saab vajaduse korral küsida täiendavaid selgitusi. See võib olla isiklik või ettevõtte e-posti aadress.

**Telefon:** telefonumber, millelt saab vajaduse korral küsida täiendavaid selgitusi. See võib olla isiklik või ettevõtte telefoninumber.

**Teine kontaktisik:** teise isiku ees- ja perekonnanimi, kellega pädev asutus võib ühendust võtta intsidendiga seotud küsimustes, kui peamine kontaktisik ei ole kättesaadav. Kui kolmas isik teatab intsidendist mõjutatud makseteenuse pakkuja nimel, tuleb märkida mõjutatud makseteenuse pakkuja intsidendi juhtimise eest vastutava / riskiosakonna või sarnase valdkonna eest vastutava isiku ees- ja perekonnanimi.

**E-post:** teise kontaktisiku e-posti aadress, millelt saab vajaduse korral küsida täiendavaid selgitusi. See võib olla isiklik või ettevõtte e-posti aadress.

**Telefon:** teise kontaktisiku telefoninumber, millelt saab vajaduse korral küsida täiendavaid selgitusi. See võib olla isiklik või ettevõtte telefoninumber.

**Aruandev üksus:** see osa tuleb täita juhul, kui kolmas isik täidab aruandluskohustusi mõjutatud makseteenuse pakkuja nimel.

**Aruandva üksuse nimi** intsidendist teatava üksuse täisnimi, nagu see on kantud kehtivasse ametlikku riiklikku äriregistrisse.

**Riiklik tunnusnumber:** unikaalne riiklik tunnusnumber, mida kasutatakse riigis, kus asub kolmas isik, intsidendist teatava äriühingu üheselt tuvastamiseks. Kui intsidendist teavitav kolmas isik on makseteenuse pakkuja, peaks unikaalne tunnusnumber olema vastava makseteenuse pakkuja unikaalne tunnusnumber, mida kasutab päritoluliikmesriigi pädev asutus oma riiklikus registris.

**Esimene kontaktisik:** intsidendist teatamise eest vastutava isiku ees- ja perekonnanimi.

**E-post:** e-posti aadress, millelt saab vajaduse korral küsida täiendavaid selgitusi. See võib olla isiklik või ettevõtte e-posti aadress.

**Telefon:** telefonumber, millelt saab vajaduse korral küsida täiendavaid selgitusi. See võib olla isiklik või ettevõtte telefoninumber.

**Teine kontaktisik:** intsidendist teatava üksuse teise isiku ees- ja perekonnanimi, kellega võib pädev asutus ühendust võtta, kui peamine kontaktisik ei ole kättesaadav.

**E-post:** teise kontaktisiku e-posti aadress, millelt saab vajaduse korral küsida täiendavaid selgitusi. See võib olla isiklik või ettevõtte e-posti aadress.

**Telefon:** teise kontaktisiku telefoninumber, millelt saab vajaduse korral küsida täiendavaid selgitusi. See võib olla isiklik või ettevõtte telefoninumber.

## A 2 - Intsidendi avastamine ja liigitamine

**Intsidendi avastamise kuupäev ja kellaaeg:** kuupäev ja kellaaeg, mil intsident esmakordselt avastati.

**Intsidendi liigitamise kuupäev ja kellaaeg:** oluliseks turva- või operatsiooniriskiintsidendi liigitamise kuupäev ja kellaaeg.

**Intsidendi avastaja:** märkige, kas intsidendi avastas makseteenuse kasutaja, makseteenuse pakkuja sisene pool (nt siseauditi üksus) või väline pool (nt teenusepakkuja). Kui intsidendi avastas keegi muu kui eespool loetletud isik, siis selgitage vastaval väljal.

**Intsidendi liik:** täpsustage, kas intsident on teile teadaolevalt ja olemasoleva teabe alusel operatsiooniriski- või turvaintsident.

**Operatsiooniriskiintsident:** intsident, mis tuleneb puudulikest või rikkega protsessidest, süsteemidest ja inimlikest vigadest või vääramatust jõust, mis mõjutavad makseteenuste terviklust, käideldavust, konfidentsiaalsust ja/või autentsust.

**Turvalisus:** volitamata juurdepääs makseteenuse pakkuja varadele, nende kasutamine, avalikustamine, katkestamine, muutmine või hävitamine, mis mõjutab makseteenuste terviklust, käideldavust, konfidentsiaalsust ja/või autentsust. See võib muu hulgas juhtuda siis, kui rikuti makseteenuse pakkuja võrgu või infosüsteemide turvalisust.

**Kriteeriumid, mille korral tuleb esitada olulise intsidendi aruanne:** täpsustage, millise kriteeriumi alusel olulise intsidendi aruanne esitatakse. Järgmiste kriteeriumite seast võib teha mitu valikut: mõjutatud tehingud, mõjutatud makseteenuse kasutajad, teenuse seisuaeg, võrgu või infosüsteemide turvalisuse

rikkumine, majandusmõju, suur, ettevõttesisene eskalatsioon, teised võimalikud mõjutatud makseteenuse pakkujad või asjakohased taristud ja/või mainemõju.

**Intsidenti lühi- ja üldkirjeldus:** selgitage lühidalt intsidenti põhipunkte, võimalikke põhjusi, vahetut mõju jne.

**Mõju teistes ELi liikmesriikides, kui mõju esineb:** selgitage lühidalt intsidenti mõju teises ELi liikmesriigis (nt makseteenuse kasutajatele, makseteenuse pakkujatele ja/või maksetaristutele). Kui see on aruande esitamise tähtaegade raames võimalik, esitage ka tõlge inglise keelde.

**Teiste asutuste teavitamine:** täpsustage, kas intsidendist on teavitatud / teavitatakse eraldiseisvas intsidentidest teavitamise raamistikus ka teisi asutusi, kui see on aruande esitamise ajal teada. Kui see on nii, täpsustage vastavad asutused.

**Esialgse aruande hilinemisega esitamise põhjused:** selgitage põhjuseid, miks vajasite intsidenti liigitamiseks üle 24 tunni aega.

## B Vahearuanne

### B 1 – Üldandmed

**Intsidenti üksikasjalikum kirjeldus:** kirjeldage intsidenti põhiomadusi, esitades teavet vähemalt konkreetse probleemi ja selle tausta kohta, ning kirjeldage intsidenti algust ja arengut ning tagajärgi, eelkõige makseteenuse kasutajatele jms. Täpsustage, kas makseteenuse kasutajaid on teavitatud, kui see on asjakohane.

**Kas see oli seotud varasema intsidenti / varasemate intsidentidega:** märkige, kas intsident on seotud varasemate intsidentidega, kui vastav teave on olemas. Kui intsident on seotud varasemate intsidentidega, täpsustage, millistega.

**Kas intsident mõjutas teisi teenuse osutajad / kolmandaid isikuid või nad olid sellesse kaasatud:** täpsustage, kas intsident mõjutas teisi teenuse osutajad / kolmandaid isikuid või nad olid sellesse kaasatud, kui vastav teave on olemas. Kui intsident mõjutas teisi teenuse osutajad / kolmandaid isikuid või nad olid kaasatud, loetlege nad ja esitage täiendavat teavet.

**Kas alustati kriisiohjega (ettevõttesisese ja/või -välise):** täpsustage, kas on alustatud (ettevõttesisese ja/või -välise) kriisiohjega. Kui kriisiohjega on alustatud, esitage täiendavat teavet.

**Intsidenti alguse kuupäev ja kellaag:** kuupäev ja kellaag, mil intsident algas, kui on teada.

**Intsidendist taastumise või eeldatava taastumise kuupäev ja kellaag:** märkige kuupäev ja kellaag, mil intsident saadi või saadakse eeldatavalt kontrolli alla ja normaalne tegevus jätkus või eeldatavalt jätkub.

**Mõjutatud funktsionaalsed valdkonnad:** tooge välja makseprotsessi samm või sammud, mida intsident mõjutas, näiteks autentimine/autoriseerimine, teabeedastus, kliiring, otsearveldus, kaudne arveldus ja muud.

**Autentimine/autoriseerimine:** menetlused, mille abil makseteenuse pakkuja saab tuvastada makseteenuse kasutaja isiku või konkreetse maksevahendi kasutamise kehtivuse, sh kasutaja isikustatud turvavolitused ja makseteenuse kasutaja (või selle kasutaja nimel tegutseva kolmanda isiku), andes oma nõusoleku vahendite ülekandmiseks.

**Teabeedastus:** teabevoog kontot teenindava makseteenuse pakkuja ning makse algatamise teenuse pakkujate, kontoteabe teenuse pakkujate, maksjate, makse saajate ja teiste makseteenuse pakkujate vaheliseks tuvastamiseks, autentimiseks, teavitamiseks ja infovahetuseks.

**Kliiring:** ülekandekorralduste edastamine ja lahendamine ning mõningatel juhtudel kinnitamine enne arveldamist, mille hulka võivad kuuluda korralduste tasaarvestamine ning lõplike arvelduspositsioonide määramine.

**Otsearveldus:** tehingu või töötlemise lõpuleviimine eesmärgiga täita osalejate kohustused vahendite ülekandmise kaudu, kui toimingu sooritab mõjutatud makseteenuse pakkuja ise.



**Kaudne arveldus:** tehingu või töötlemise lõpuleviimine eesmärgiga täita osalejate kohustused vahendite ülekandmise kaudu, kui toimingut sooritab mõjutatud makseteenuse pakkuja nimeline makseteenuse pakkuja.

**Muu:** mõjutatud tegevusvaldkond on muu kui eespool loetletud. Täiendavad üksikasjad tuleb märkida vabatekstiväljale.

**Varasemates aruannetes tehtud muudatused:** tooge välja sama intsidendiga seotud varasemates aruannetes esitatud teabes tehtud muudatused (nt esialgses või vahearuandes, kui see esitati).

## B 2 – Intsidendi liigitamine / intsidendi teave

**Mõjutatud tehingud:** Makseteenuse pakkujad peaksid välja tooma, mis piirmääradeni intsident tõenäoliselt jõuab ning asjaomased arvanded: mõjutatud tehingute arv, mõjutatud tehingute osakaal samade intsidendist mõjutatud makseteenustega teostatud maksetehingute arvust ning tehingute koguväärtus. Makseteenuse pakkujad peaksid esitama nende muutujate konkreetset väärtused, mis võivad olla tegelikud arvud või hinnangud. Üldiselt peaksid makseteenuse pakkujad mõistma „mõjutatud tehingutena“ kõiki riigisiseseid ja piiriüleseid tehinguid, mida intsident on mõjutanud või tõenäoliselt otseselt või kaudselt mõjutab, ning eriti tehinguid, mida ei õnnestunud algatada ega töödelda, mille makseteateise sisu muudeti ja mis telliti pettuse teel (olenemata sellest, kas vahendid saadi tagasi või mitte). Lisaks peaksid makseteenuse pakkujad arvestama maksetehingute tavatasemena aasta keskmist taset igapäevaste riigisiseste ja piiriüleste maksetehingute korral, mis sooritati samade makseteenustega, mida intsident mõjutas, võttes arutuste võrdlusperioodiks eelmise aasta. Kui makseteenuse pakkujad ei pea seda väärtust tüüpiliseks (nt hooajalisuse tõttu), tuleb kasutada muud iseloomulikumat mõõdikut ning esitada pädevale asutusele meetodi aluseks olevad põhjendused vormi väljal „Märkused“. Kui intsident mõjutas maksetehinguid, mis tehti eurost erinevates valuutades, peaksid makseteenuse pakkujad piirmäärade arvutamisel ja mõjutatud tehingute väärtusest teatamisel eurost erinevas valuutas tehingute summa eurosse konverteerima, kasutades intsidendi aruande esitamisele eelnenu päeva EKP päevast viitekurssi.

**Mõjutatud makseteenuse kasutajad:** Makseteenuse pakkujad peaksid märkima, mis piirmäärad intsident saavutas või tõenäoliselt saavutab ja asjaomased arvanded: mõjutatud makseteenuse kasutajate arv kokku ja mõjutatud makseteenuse kasutajate osakaal makseteenuse kasutajate koguarvust. Makseteenuse pakkujad peaksid esitama nende muutujate konkreetset väärtused, mis võivad olla tegelikud arvud või hinnangud. Makseteenuse pakkujad peaksid mõistma „mõjutatud makseteenuse kasutajatena“ kõiki kliente (riigisiseseid ja välisriikide kliente, tarbijaid ja juriidilisi isikuid), kellel on leping mõjutatud makseteenuse pakkujaga, kes tagab neile juurdepääsu mõjutatud makseteenusele, ning kes on kannatanud või tõenäoliselt kannatavad intsidendi tagajärgede all. Makseteenuse pakkujad peaksid varasemale tegevusele tuginevate hinnangute alusel kindlaks tegema makseteenuse kasutajate arvu, kes võisid kasutada makseteenust intsidendi kestuse ajal. Konsolideerimisgruppide korral peaks iga makseteenuse pakkuja arvestama ainult enda makseteenuse kasutajaid. Kui makseteenuse pakkuja osutab teenuseid teistele makseteenuse pakkujatele, peaks ta arvestama ainult enda makseteenuse kasutajaid (kui need on olemas), ning neid teenuseid kasutavad makseteenuse pakkujad peaksid hindama intsidenti enda makseteenuse kasutajate suhtes. Lisaks peaksid makseteenuse pakkujad lugema makseteenuse kasutajate koguarvuks intsidendi toimumise ajal nendega lepingulises suhtes olnud nende riigisiseste ja piiriüleste makseteenuse kasutajate koondarvu, kellel on juurdepääs mõjutatud makseteenusele, sõltumata nende suurusest või sellest, kas neid loetakse makseteenuse aktiivseteks või passiivseteks kasutajateks (või teise võimalusena kõige viimast kättesaadavat arvu).

**Võrgu või infosüsteemide turvalisuse rikkumine:** Makseteenuse pakkujad peaksid välja selgitama, kas kuritahtlik tegevus ohustas makseteenuste osutamise seotud võrgu või infosüsteemide (sh andmete) käideldavust, autentsust, puutumatumust või konfidentsiaalsust.

**Teenuse seisuaeg:** Makseteenuse pakkujad peaksid märkima, kas intsident saavutas või tõenäoliselt saavutab teatud piirmäära, ja seonduva väärtuse: teenuse kogu seisuaaja. Makseteenuse pakkujad peaksid esitama selle muutuja konkreetseid väärtused, mis võivad olla tegelikud arvud või hinnangud. Makseteenuse pakkujad peaksid arvestama ajavahemikku, mil makseteenuse osutamisega seotud mis tahes toiming, töötlemine või kanal on või tõenäoliselt on katkenud, mis seega takistab i) makseteenuse algatamist ja/või täitmist ja/või ii) juurdepääsu maksekontole. Makseteenuse pakkujad peaksid arvestama teenuse seisuaega selle algushetkest, samuti tuleks arvestada nii ajavahemikke, mil nad on avatud tegevuseks (vajalik makseteenuste teostamiseks), kui ka ajavahemikke, mil nad on suletud, ning hooldusperioode, kui need on asjakohased ja kohaldatavad. Kui makseteenuse pakkujad ei suuda teha kindlaks teenuse seisuaaja algust, peaksid nad erandkorras arvestama teenuse seisuaega alates intsidendi avastamisest.

**Majandusmõju:** Makseteenuse pakkujad peaksid märkima, kas intsident saavutas või tõenäoliselt saavutab teatud piirmäära, ja seonduvad väärtused: otsesed ja kaudsed kulud. Makseteenuse pakkujad peaksid esitama nende muutujate konkreetseid väärtused, mis võivad olla tegelikud arvud või hinnangud. Makseteenuse pakkujad peaksid arvestama intsidendiga otseselt ja kaudselt seotud kulusid. Muu hulgas peaksid makseteenuse pakkujad arvestama sundvõõrandatud vahendeid või vara, riistvara või tarkvara asenduskulusid, muid kohtuekspertiiside või parandusmeetmete kulusid, lepingukohustuste mittetäitmise trahve, sanktsioone, väliseid kohustusi ja kaotatud tulu. Kaudsete kuludena peaksid makseteenuse pakkujad arvestama ainult kulusid, mis on juba teada või mille realiseerumine on väga tõenäoline. Kui kulud kanti eurost erinevates valuetades, peaksid makseteenuse pakkujad piirmäärade arvutamisel ja majandusmõju väärtusest teatamisel eurost erinevas valuetas kulude summa eurodesse konverteerima, kasutades intsidendi aruande esitamisele eelnenud päeva EKP päevast viitekurssi.

**Otsesed kulud:** kulud (eurodes), mis tekkisid intsidendi tõttu otsese kuluna, sh intsidendi kõrvaldamise kulud (nt sundvõõrandatud vahendid või vara, riistvara või tarkvara asenduskulud, lepingukohustuste mittetäitmise trahvid).

**Kaudsed kulud:** kulud (eurodes), mille intsident põhjustas kaudselt (nt kliendile heastamise/hüvitamise kulud, võimalikud õiguskulud).

**Suur ettevõttesisene eskalatsioon:** Makseteenuse pakkujad peaksid kaalutlema, kas EBA IKT- ja turvariskide ohjamise suunistes määratletud juhtorganit on kooskõlas EBA IKT- ja turvariskide ohjamise suuniste 60. punkti alapunktiga d maksetega seotud teenustele avaldunud mõju tõttu intsidendist teavitatud või tõenäoliselt teavitatakse väljaspool perioodilise teavitamise korda ja pidevalt terve intsidendi kestuse jooksul. Lisaks peaksid makseteenuse pakkujad kaalutlema, kas seoses intsidendi mõjuga makseteenustele käivitus või tõenäoliselt käivitub kriisiolukord.

**Teised võimalikud mõjutatud makseteenuse pakkujad või asjakohased taristud:** makseteenuse pakkujad peaksid hindama intsidendi mõju finantsturile, mida mõistetakse finantsturu taristutena ja/või makseskeemidena, mis toetavad neid ja teisi makseteenuse pakkujaid. Makseteenuse pakkujad peaksid eelkõige hindama, kas intsident kordus või tõenäoliselt kordub teiste makseteenuse pakkujatega, kas see on mõjutanud või tõenäoliselt mõjutab finantsturu taristute sujuvat toimimist ning kas see ohustas või tõenäoliselt ohustab finantssüsteemi kindlust tervikuna. Makseteenuse pakkujad peaksid meeles pidama eri mõõtmeid, näiteks kas mõjutatud komponent/tarkvara on ettevõttesisene või üldiselt kättesaadav, kas ohustatud võrk on ettevõttesisene või -väline ning kas makseteenuse pakkuja on katkestanud või tõenäoliselt katkestab oma kohustuste täitmise finantsturu taristutes, kuhu ta kuulub.

**Mainemõju:** makseteenuse pakkujad peaksid arvestama nähtavuse ulatust, mille intsident nende parima teadmise kohaselt turul saavutas või tõenäoliselt saavutab. Makseteenuse pakkujad peaksid eelkõige arvestama, et intsidendi poolt ühiskonnale tekitatava kahju tõenäosus näitab ilmekalt nende maine kahjustamise võimalikkust. Makseteenuse pakkujad peaksid võtma arvesse, kas i) makseteenuse kasutajad ja/või teised makseteenuste osutajad on kaevanud intsidendi negatiivse mõju üle, ii) intsident

on mõjutanud nähtavat makseteenusega seotud protsessi ja seda kajastatakse tõenäoliselt või on juba kajastatud meedias (peale tavapärase meedia, nt ajalehtede, ka blogides, suhtlusvõrgustikes jne), ent meedias kajastamine ei tähenda selles kontekstis jälgijate paari negatiivset kommentaari, tegemist peab olema arvestatava kajastuse või olulise negatiivsete märkuste/hoiatuste arvuga), iii) lepingulised kohustused on jäänud või jäävad tõenäoliselt täitmata, mille tõttu algatakse makseteenuse pakkuja vastu kohtuasju, iv) õigusaktide nõudeid ei ole täidetud, mille tõttu kohaldatakse järelevalvemeetmeid või sanktsioone, mille teave tehakse tõenäoliselt avalikkusele kättesaadavaks, või v) sarnast tüüpi intsidente on ka varem esinenud.

### B 3 – Intsidendi kirjeldus

**Intsidendi liik:** operatsiooniriski- või turvaintsident. Täiendav selgitus esitatakse esialgse aruande vastaval väljal.

**Intsidendi põhjus:** märkige intsidendi põhjus, või kui see ei ole veel teada, siis kõige tõenäolisem põhjus. Valida võib mitu erinevat põhjust.

**Põhjust uuritakse:** märgistage see ruut juhul, kui põhjus ei ole hetkel teada.

**Kuritahtlik tegevus:** tahtlikult makseteenuse pakkuja vastu suunatud tegevused. Need hõlmavad ründekoodi, teabe kogumist, sissetunge, hajus-/ummistusrünnet (DDoS), tahtlikku ettevõttesisest tegevust, tahtlikku asutusevälist füüsilist kahju, teabesisu turvet, pettust ja muud. Vt lisateave vormi osas C 2.

**Protsessi rike:** intsidendi põhjustasid puudulikult väljatöötatud või rakendatud makseprotsess, protsessi juhttoimingud ja/või tugiprotsessid (nt muutmise/migratsiooni, katsetamise, konfigureerimise, suutlikkuse tagamise, jälgimise protsess).

**Süsteemi rike:** intsidendi põhjus on seotud maksetoimingut toetavate süsteemide, võrkude, taristute ja andmebaaside puuduliku väljatöötamise, käitamise, komponentide, tehniliste nõuete, integreerimise või keerukusega.

**Inimlik eksimus:** intsidendi põhjustas tahtmatu inimlik eksimus, kas maksemenetluse osana (nt vale maksete pakkkfaili üleslaadimine maksesüsteemi) või sellega muul viisil seoses (nt elektrikatkestuse tõttu pandi maksetehing ootele).

**Välissündmused:** põhjus on seotud sündmustega, mille üle puudub organisatsioonil üldjuhul otsene kontroll (nt loodusõnnetused, tehnilise teenuse osutaja rike).

**Muu:** intsidendi põhjus on muu kui eespool loetletud. Täiendavad üksikasjad tuleb märkida vabatekstiväljale.

**Kas intsident mõjutas teid otseselt või kaudselt teenusepakkuja kaudu?:** Märkige, kas intsident oli otse makseteenuse pakkuja vastu suunatud või mõjutas teda kaudselt kolmanda isiku kaudu (kui see teave on olemas). Kaudse mõju korral märkige teenusepakkuja(te) nimi (nimed).

### B 4 – Intsidendi mõju

**Üldmõju:** märkige, mis valdkondi operatsiooniriski- või turvaintsident mõjutas. Valida võib mitu erinevat põhjust.

**Terviklus:** varade (sh andmete) täpsus ja terviklus on kaitstud.

**Käideldavus:** maksetega seotud teenused on makseteenuse kasutajatele kättesaadavad ja kasutatavad vastavalt eelnevalt kindlaks määratud aktsepteeritavatele tasemetele.

**Konfidentsiaalsus:** teavet ei tehta kättesaadavaks ega avalikustata volitamata isikutele, üksustele ega protsessidele.

**Autentsus:** allikas on sama, mis see väidab end olevat.

**Mõjutatud kommertskanalid:** märkige makseteenuse kasutajatega suhtlemiseks kasutatav suhtluskanal või -kanalid, mida intsident mõjutas. Valida võib mitu vastusevarianti.

**Filiaalid:** tegevuskoht (muu kui peakontor), mis on makseteenuse pakkuja osa, millel puudub juriidilise isiku staatus ning mis sooritab otseselt mõningaid või kõiki makseteenuse pakkuja

äritegevusega seotud tehinguid. Kõiki tegevuskohti, mille ühes liikmesriigis on asutanud teises liikmesriigis asuva peakontoriga makseteenuse pakkuja, käsitatakse ühe filiaalina.

**E-pangandus:** finantstehingute sooritamine internetis arvutite abil.

**Telefonipangandus:** finantstehingute sooritamine telefonide abil.

**Mobiilipangandus:** finantstehingute sooritamine nutitelefonis või sarnases seadmes spetsiaalse pangarakenduse abil.

**Sularahaautomaadid:** elektromehaanilised seadmed, millega makseteenuse kasutajad saavad teha oma kontodelt sularahaväljavõtteid ja/või kasutada muid teenuseid.

**Müügikoht:** kaupleva füüsiline tegevuskoht, kus maksetehing algatatakse.

**E-kaubandus:** maksetehing algatatakse virtuaalses müügikohas (nt interneti teel algatatavad maksed, milleks kasutatakse krediitkorraldusi, maksekaarte, e-raha e-raha kontode vahelist ülekandmist).

**Muu:** mõjutatud äritegevuse kanal on muu kui loetletud eespool. Täiendavad üksikasjad tuleb märkida vabatekstiväljale.

**Mõjutatud makseteenused:** märkige makseteenused, mis ei toimi intsidendi tagajärjel nõuetekohaselt. Valida võib mitu vastusevarianti.

**Sularaha ülekanne maksekontole:** sularaha andmine makseteenuse pakkujale selle krediteerimiseks maksekontole.

**Sularaha väljavõtt maksekontolt:** makseteenuse kasutaja taotlus makseteenuse pakkujale sularaha saamiseks ja tema maksekonto debiteerimiseks vastava summa võrra.

**Maksekonto teenindamiseks vajalikud toimingud:** toimingud, mida on vaja maksekonto aktiveerimiseks, deaktiveerimiseks ja/või haldamiseks (nt avamine, blokeerimine).

**Makseinstrumentide taotlemine:** makseteenus, mis sisaldab makseteenuse pakkuja ja makse saaja lepingut maksetehingute kinnitamiseks ja töötlemiseks, mille tulemusena kantakse vahendid üle makse saajale.

**Krediitkorraldused:** makseteenus, millega makseteenuse pakkuja, kelle juures asub maksja maksekonto, krediteerib makse saaja maksekontot maksetehingu või järjestikuste maksetehingutega maksja maksekontolt maksja antud juhise alusel.

**Otsekorraldused:** makseteenus, millega debiteeritakse maksja maksekontot, millelt makse saaja on algatanud maksetehingu, makse saajale, makse saaja makseteenuse pakkujale või maksja enda makseteenuse pakkujale, lähtudes maksja poolt antud nõusolekust.

**Kaardimaksed:** maksekaardiskeemi taristul ja ärieeskirjadel põhinev makseteenus maksetehingu tegemiseks kaardi, sidevahendi, digitaalse või IT-seadme või tarkvaraga, kui selle tulemuseks on deebet- või krediitkaarditehing. Kaardipõhiste maksetehingute hulka ei kuulu muudel makseteenustel põhinevad tehingud.

**Makseinstrumentide väljastamine:** makseteenus, mille kaudu makseteenuse pakkuja annab makseteenuse pakkuja ja maksja vahel sõlmitud lepingu alusel maksja käsutusse makseinstrumenti maksja maksetehingute algatamiseks ja töötlemiseks.

**Rahasiire:** makseteenus, mille kaudu saadakse maksjalt rahalisi vahendeid ilma maksja või makse saaja nimel maksekontosid loomata ja mille eesmärk on vastava summa ülekandmine makse saajale või makse saaja nimel tegutsevatele teistele makseteenuse pakkujale ja/või mille kaudu vahendid saadakse makse saaja nimel või tehakse makse saajale kättesaadavaks.

**Makse algatamise teenused:** makseteenused maksekorralduse algatamiseks makseteenuse kasutaja taotlusel teise makseteenuse pakkuja juures asuvale maksekontole.

**Kontoteabe teenused:** veebipõhised makseteenused konsolideeritud teabe andmiseks makseteenuse kasutaja ühe või mitme maksekonto kohta makseteenuse teise või mitme pakkuja juures.

## B 5 – Intsidendi mõju leevendamine

**Mis meetmeid on seni rakendatud või kavatsetakse rakendada intsidendist taastumiseks?:** Esitage üksikasjalik teave meetmete kohe, mida on rakendatud või mida kavatsetakse rakendada ajutiselt intsidendi lahendamiseks.

**Kas talitluspidevuse ja/või taasteplaani on käivitatud:** märkige, kas see on toimunud, ja kui see nii on, esitage juhtunu kohta kõige asjakohasemad andmed (st millal need käivitati ja milles need seisnesid).

## C – Lõpparuanne

### C 1 – Üldandmed

**Esialgses aruandes ja vahearuandes/vahearuanetes esitatud teabe uuendamine** (kokkuvõte): esitage intsidendi kohta lisateavet, sh teavet vahearuandes esitatud teabe muutumise kohta. Lisage ka igasugune muu asjakohane teave.

**Kas kõik algsed kontrollid on jälle kasutusel?:** Märkige, kas makseteenuse pakkuja pidi intsidendi ajal mis tahes ajahetkel teatud algsed kontrollid tühistama või neid nõrgendama. Kui see nii on, täpsustage, kas kõik algsed kontrollid on jälle kasutusel, ja kui ei ole, selgitage vabatekstiväljal, millised algsed kontrollid ei ole veel kasutusel ja kui pikka perioodi on vaja nende taastamiseks.

### C 2 – Juurpõhjuse analüüs ja järeltoimingud

**Mis oli juurpõhjus, kui see on juba teada:** märkige intsidendi põhjus, või kui see ei ole veel teada, siis kõige tõenäolisem põhjus. Valida võib mitu erinevat põhjust. (NB! Juurpõhjust tuleks eristada intsidendi mõjust.)

**Kuritahtlik tegevus:** ettevõttesisesed või -välised tahtlikult makseteenuse pakkuja vastu suunatud tegevused. Need jaotuvad järgmisteks kategooriateks:

**Ründekood:** nt viirus, ussviirus, Trooja hobune, nuhkvara.

**Teabe kogumine:** nt skaneerimine, nuuskimine, sotsiaalne manipulatsioon.

**Sissetungid:** nt privilegeeritud konto kahjustamine, tavakonto kahjustamine, rakenduse kahjustamine, robot.

**Hajus-/ummistusrünne:** katse muuta veebiteenus kättesaamatuks, koormates selle üle eri allikatest pärit võrguliiklusega.

**Tahtlik ettevõttesisene tegevus:** nt sabotaaž, vargus.

**Tahtlik asutuseväline füüsiline kahju:** nt sabotaaž, ruumide/andmekeskuste füüsiline ründamine.

**Teabesisu turve:** omavoliline juurdepääs teabele, teabe omavoliline muutmine.

**Pettus:** vahendite, autoriõiguste omavoliline kasutamine, teesklusrünne, andmepüük.

**Muu (täpsustage):** intsidendi põhjus on muu kui eespool loetletud. Täiendavad üksikasjad tuleb märkida vabatekstiväljale.

**Protsessi rike:** intsidendi põhjustasid puudulikult väljatöötatud või rakendatud makseprotsess, protsessi juhttoimingud ja/või tugiprotsessid (nt muutmise/migratsiooni, katsetamise, konfigureerimise, suutlikkuse tagamise, jälgimise protsess). Need jaotuvad järgmisteks kategooriateks:

**Ebapiisav järelevalve ja ohje:** nt seoses operatsioonide juhtimise, sertifikaatide lõpptähtaegade, litsentside lõpptähtaegade, turvapaikade lõpptähtaegade, kindlaksmääratud maksimumväärtuste, andmebaaside täitumise tasemete, kasutajaõiguste haldamise, topeltkontrolli põhimõttega.

**Teavitusprobleemid:** nt turuosaliste vahelised või organisatsioonisesed.

Ebaõige käitamine: nt sertifikaate ei vahetata, vahemälu on täis.

**Ebapiisav muutuste juhtimine:** nt tuvastamata konfiguratsioonivead, kasutuselevõtt, sh uuendused, hooldusprobleemid, ootamatud vead.

**Ettevõttesiseste menetluste ja dokumentide ebapiisavus:** nt funktsioonide, protsesside ja rikete esinemisega seotud ebapiisav läbipaistvus, dokumentide puudumine.

**Taasteprobleemid:** nt ettenägematute olukordade juhtimine, ebapiisav liiasus.

**Muu (täpsustage):** intsidendi põhjus on muu kui eespool loetletud. Täiendavad üksikasjad tuleb märkida vabatekstiväljale.

**Süsteemi töötõrge:** intsidendi põhjus on seotud maksetoimingut toetavate süsteemide, võrkude, taristute ja andmebaaside puuduliku väljatöötamise, käitamise, komponentide, tehniliste nõuete, integreerimise või keerukusega. Need jaotuvad järgmisteks kategooriateks:

**Riistvara rike:** protsesse käitava ja/või makseteenuse pakkujatele nende maksetega seotud tegevuse teostamiseks vajalikke andmeid salvestava füüsilise tehnoloogiaseadme rike (nt kõvaketaste, andmekeskuste, muu taristu rikked).

**Võrgurike:** makseprotsessi käigus andmete ja teabe vahetamist võimaldavate (nt internetikaudsete) avalik-õiguslike või eratelekommunikatsioonivõrkude rike.

**Andmebaasi probleemid:** andmestruktuur, mis säilitab maksetehingute teostamiseks vajalikke isiku- ja makseandmeid.

**Tarkvara/rakenduse rike:** makseteenuse pakkuja makseteenuste osutamist toetavate programmide, operatsioonisüsteemide jms rike (nt talitlushäired, tundmatud funktsioonid).

**Füüsiline kahju:** nt ebasobivatest tingimustest, ehitustöödest tingitud tahtmatu kahju.

**Muu (täpsustada):** intsidendi põhjus on muu kui eespool loetletud. Täiendavad üksikasjad tuleb märkida vabatekstiväljale.

**Inimlik eksimus:** intsidendi põhjustas tahtmatu inimlik eksimus, kas maksemenetluse osana (nt vale maksete pakkfai üleslaadimine maksesüsteemi) või sellega muul viisil seoses (nt tahtmatu elektrikatkestuse tõttu pandi maksetoiming ootele). Need jaotuvad järgmisteks kategooriateks:

**Tahtmatud:** nt vead, eksimused, tegematajätmised, kogemuste ja teadmiste vähesus.

**Tegevusetus:** nt oskuste, teadmiste, kogemuste, teadlikkuse vähesuse tõttu.

**Ebapiisavad ressursid:** nt ebapiisavad inimressursid, personali kättesaadavus.

**Muu (täpsustada):** intsidendi põhjus on muu kui loetletud eespool. Täiendavad üksikasjad tuleb märkida vabatekstiväljale.

**Välissündmused:** põhjus on seotud sündmustega, mille üle organisatsioonil puudub üldjuhul kontroll. Need jaotuvad järgmisteks kategooriateks:

**Tarnija/ tehnilise teenuse osutaja rike:** nt elektrikatkestus, internetiühenduse katkestus, juriidilised probleemid, ärialased probleemid, teenuse sõltuvus.

**Vääramatu jõud:** nt elektrikatkestus, tulekahjud, loodusõnnetused, näiteks maavärinad, üleujutused, rohked sademed, tugev tuul.

**Muu (täpsustada):** intsidendi põhjus on muu kui loetletud eespool. Täiendavad üksikasjad tuleb märkida vabatekstiväljale.

**Muu:** intsidendi põhjus on muu kui eespool loetletud. Täiendavad üksikasjad tuleb märkida vabatekstiväljale.

**Muu asjaomane teave juurpõhjuse kohta:** esitage juurpõhjuse kohta lisaandmeid, sealhulgas juurpõhjuse analüüsi alusel tehtud esialgsed järeldused.

**Parandusmeetmed või kavandatavad meetmed intsidendi kordumise takistamiseks tulevikus, kui on juba teada:** kirjeldage peamisi meetmeid, mida on juba rakendatud või mida kavatakse rakendada intsidendi kordumise takistamiseks tulevikus.

### C 3 – Lisateave

**Kas intsidendi teavet on jagatud teiste makseteenuse pakkujatega teavitamise eesmärgil:** andke ülevaade makseteenuse pakkujatest, kellega on (ametlikult või mitteametlikult) ühendust võetud intsidendi lühiülevaate andmiseks, märkides teavitatud makseteenuse pakkujate andmed, jagatud teabe ja teabe jagamise põhjused.

**Kas makseteenuse pakkuja suhtes on rakendatud õiguslikke meetmeid:** märkige, kas lõpparuande täitmise ajal on makseteenuse pakkuja suhtes rakendatud õiguslikke meetmeid (nt algatatud kohtuasi või võetud ära tegevusluba).

**Võetud meetmete tulemuslikkuse hindamine:** lisage võimaluse korral intsidendi käigus võetud meetmete tõhususele antud enesehindang, sealhulgas intsidendist saadud kogemuste kirjeldus.