EBA/GL/2017/10

19/12/2017

Suunised

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

1. Järgimis- ja aruandluskohustus

Käesolevate suuniste staatus

1. Käesolev dokument sisaldab määruse (EL) nr 1093/2010 [1] artikli 16 kohaselt väljastatud suuniseid. Määruse (EL) nr 1093/2010 artikli 16 lõike 3 kohaselt peavad pädevad asutused ja finantseerimisasutused võtma mis tahes meetmeid, et suuniseid järgida.

2. Suunistes esitatakse Euroopa Pangandusjärelevalve seisukoht nõuetekohase järelevalvetava kohta Euroopa Finantsjärelevalve Süsteemis, ehk kuidas tuleks liidu õigust konkreetses valdkonnas kohaldada. Suuniste adressaadiks olevad määruse (EL) nr 1093/2010 artikli 4 punktis 2 määratletud pädevad asutused peaksid suuniseid järgima, kaasates need sobival viisil oma järelevalvetavadesse (nt muutes oma õigusraamistikku või järelevalvemenetlusi) ka siis, kui suunised on mõeldud eelkõige finantseerimisasutustele.

Aruandluskohustus

3. Määruse (EL) nr 1093/2010 artikli 16 lõike 3 kohaselt peavad pädevad asutused teatama EBA-le 19/02/2018, kas nad järgivad või kavatsevad järgida kõnealuseid suuniseid, või vastasel juhul mittejärgimise põhjused. Kui selleks tähtajaks teadet ei saada, peab EBA pädevat asutust nõudeid mitte täitvaks. Teated tuleks saata EBA veebisaidil avaldatud vormil aadressil compliance@eba.europa.eu, märkides viite EBA/GL/2017/10. 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 teada anda.

4. Kooskõlas EBA määruse artikli 16 lõikega 3 avaldatakse teated Euroopa Pangandusjärelevalve veebilehel.

[1] Euroopa Parlamendi ja nõukogu määrus (EL) nr 1093/2010, 24. november 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 Euroopa Pangandusjärelevalvele antud volitustel.

6. Eelkõige täpsustatakse suunistes makseteenuse pakkujatele oluliste operatsiooniriski- või turvaintsidentide liigitamise kriteeriumid, samuti eespool nimetatud direktiivi artikli 96 lõikes 1 sätestatud vorm ja protseduurid, mida tuleb järgida intsidentidest päritoluliikmesriigi pädevale asutusele teatamisel.

7. Lisaks käsitletakse suunistes viise, kuidas need pädevad asutused peaksid hindama intsidendi asjakohasust ja vastavalt nimetatud direktiivi artikli 96 lõikele 2 jagama intsidendiaruande üksikasju 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 teatamise suhtes vastavalt direktiivi (EL) 2015/2366 artiklile 96.

10. Suuniseid kohaldatakse kõigi „olulise operatsiooniriski- või turvaintsidendi“ määratluse alla kuuluvate intsidentide suhtes, mis hõlmab 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 ettevõte) või kaudselt (makseteenuse pakkuja suutlikkus jätkata makseteenuste osutamist on intsidendi tulemusena muul viisil ohustatud).

Adressaadid

12. 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.

13. 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

14. Kui ei ole sätestatud teisiti, on määruses (EL) 2015/2366 kasutatud ja määratletud mõistetel siin suunistes sama tähendus. Peale selle kasutatakse siin suunistes järgmisi mõisteid.

Operatsiooniriski- või turvaintsident	Sündmus või mitu seotud sündmust, mida makseteenuse pakkuja ei ole kavandanud, mis kahjustavad või tõenäoliselt kahjustavad maksetega seotud teenuste terviklust, käideldavust, konfidentsiaalsust, autentsust ja/või talitluspidevust.
Terviklus	Varade (sh andmete) täpsus ja terviklus on kaitstud.
Käideldavus	Maksetega seotud teenused on makseteenuse kasutajatele kättesaadavad ja kasutatavad.
Konfidentsiaalsus	Teavet ei tehta kättesaadavaks ega avalikustata volitamata isikutele, üksustele ega protsessidele.
Autentsus	Allikas on sama, mis see väidab end olevat.
Talitluspidevus	Organisatsiooni protsessid, toimingud ja varad, mida on vaja maksetega seotud teenuste osutamiseks, on täielikult juurdepääsetavad ning toimivad heakskiidetud eelmääratletud tasemetel.
Maksetega seotud teenused	Mis tahes äritegevus direktiivi (EL) 2015/2366 artikli 4 punkti 3 tähenduses ning kõik makseteenuste osutamiseks vajalikud tehnilise toe toimingud.

3. Rakendamine

Kohaldamise alguskuupäev

15. Käesolevaid suuniseid kohaldatakse alates 13. jaanuarist 2018.

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 turvaintsidendid, mis vastavad

a. vähemalt ühele „kõrgema mõjutaseme“ kriteeriumile või

b. vähemalt kolmele „madalama mõjutaseme“ kriteeriumile,

nagu on sätestatud suuniste punktis 1.4 ning järgides nendes suunistes sätestatud hindamist.

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

i. Mõjutatud tehingud

Makseteenuse pakkujad peaksid määrama mõjutatud tehingute koguväärtuse ning kahjustatud maksete arvu protsendina maksetehingute tavatasemest, mis tehti koos mõjutatud makseteenustega.

ii. Mõjutatud makseteenuse kasutajad

Makseteenuse pakkujad peaksid määrama mõjutatud makseteenuse kasutajate absoluutarvu ja suhtelise arvu makseteenuse kasutajate koguarvu protsendina.

iii. Teenuse seisuaeg

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

iv. Majandusmõju

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

v. Suur ettevõttesisene eskalatsioon

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

vi. Teised võimalikud mõjutatud makseteenuse pakkujad või asjakohased taristud

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

vii. Mõju mainele

Makseteenuse pakkujad peaksid määrama, 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 metoodikale.

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 makseteatise sisu muudeti ja mis telliti pettuse teel (olenemata sellest, kas vahendid on tagasi saadud või mitte).

Lisaks peaksid makseteenuse pakkujad mõistma maksetehingute tavatasemena aasta keskmist taset igapäevaste riigisiseste ja piiriüleste maksetehingute korral, mis on tehtud koos samade makseteenustega, mida intsident mõjutas, võttes arvutuste võrdlusperioodiks eelmise aasta. Kui makseteenuse pakkujad ei pea seda suurust tüüpiliseks (nt hooajalisuse tõttu), tuleb kasutada muud iseloomulikumat suurust ning esitada pädevale asutusele meetodi aluseks olevad põhjendused vormi vastaval väljal (vt 1. 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 on kannatanud või tõenäoliselt kannatavad intsidendi tagajärgede tõttu. Makseteenuse pakkujad peaksid määrama varasemal tegevusel tuginevate hinnangute abil makseteenuse nende kasutajate arvu, kes võisid kasutada makseteenust intsidendi kestuse ajal.

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

Lisaks peaksid makseteenuse pakkujad pidama 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).

iii. Teenuse seisuaeg

Makseteenuse pakkujad peaksid arvestama ajavahemikku, mil igasugune makseteenuse osutamisega seotud toiming, töötlemine või kanal on või on tõenäoliselt maas, 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 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 teenuse seisuaja algust, peaksid nad erandkorras arvestama teenuse seisuaega alates selle avastamisest.

iv. 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.

v. *Suur ettevõttesisene eskalatsioon*

Makseteenuse pakkujad peaksid kaalutlema, kas seoses intsidendi mõjuga makseteenustele on intsidendist teavitatud või tuleks tõenäoliselt teavitada IT-juhti (või sarnasel ametikohal olevat isikut) väljaspool korralise teavitamise korda ning pidevalt kogu intsidendi kestuse ajal. Lisaks peaksid makseteenuse pakkujad kaalutlema, kas seoses intsidendi mõjuga makseteenustele käivitus või tõenäoliselt käivitub kriisiolukord.

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

Makseteenuse pakkujad peaksid hindama intsidendi mõju finantsturule, mida mõistetakse finantsturu taristutena ja/või kaardimakseskeemidena, mis toetavad neid ja teisi makseteenuse pakkujaid. Makseteenuse pakkujad peaksid eelkõige hindama, kas intsident kordus või tõenäoliselt kordub teiste makseteenuse pakkujate korral, kas see on mõjutanud või tõenäoliselt mõjutab finantsturu taristute sujuvat toimimist ning kas see ohustas või tõenäoliselt ohustab finantssüsteemi häireteta toimimist 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.

vii. *Mõju mainele*

Makseteenuse pakkujad peaksid arvestama nähtavuse ulatust, mille intsident on nende parima teadmise kohaselt turul saavutanud 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) intsident on mõjutanud nähtavat protsessi ning seda võidakse

kajastada või seda on juba kajastatud meedias (peale tavapärase meedia, nt ajalehtede, ka blogides, suhtlusvõrgustikes jne); ii) õigusaktidest tulenevad kohustused on jäetud täitmata või jäetakse tõenäoliselt täitmata; iii) rikkumiste eest on kohaldatud või tõenäoliselt kohaldatakse sanktsioone või iv) sarnane intsident on toimunud ka varem.

1.4. Makseteenuse pakkujad peaksid intsidendi hindamisel määrama iga üksikkriteeriumi korral, kas asjakohased tabeli 1 läved on saavutatud või saavutatakse tõenäoliselt enne intsidendi lahendamist.

Tabel 1. Läved

Kriteerium	Madalam mõjutase	Kõrgem mõjutase
Mõjutatud tehingud	> 10% makseteenuse pakkuja tehingute tavamäärast (tehingute arvu järgi) **ning** > 100 000 eurot	> 25% makseteenuse pakkuja tehingute tavamäärast (tehingute arvu järgi) **või** > 5 miljonit eurot
Mõjutatud makseteenuse kasutajad	> 5000 **ning** > 10% makseteenuse pakkuja makseteenuse kasutajatest	> 50 000 **või** > 25% makseteenuse pakkuja makseteenuse kasutajatest
Teenuse seisuaeg	> 2 tundi	Ei kohaldata
Majandusmõju	Ei kohaldata	> *max.* (0,1% esimese taseme omavahenditest,* 200 000 eurot) **või** > 5 miljonit 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
Mõju mainele	Jah	Ei kohaldata

* Esimese taseme omavahendid on määratletud Euroopa Parlamendi ja nõukogu 26. juuni 2013. aasta määruse (EL) nr 575/2013 (krediidiasutuste 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.

2. suunis. Teavitamisprotsess

2.1. Makseteenuse pakkujad peaksid koguma kogu asjakohase teabe, koostama 1. lisa vormi kohase intsidendiaruande ning esitama selle päritoluliikmesriigi pädevale asutusele. Makseteenuse pakkujad peaksid täitma vormi vastavalt 1. lisa juhistele.

2.2. Makseteenuse pakkujad peaksid kasutama sama vormi pädeva asutuse teavitamisel kogu intsidendi kestuse jooksul (esialgseteks, vahe- ja lõpparuanneteks, nagu on kirjeldatud punktides 2.7–2.21). Makseteenuse pakkujad peaksid täitma vormi järk-järgult nii hästi kui võimalik vastavalt sisejuurdluses selgunud teabele.

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 edastama päritoluliikmesriigi pädevale asutusele mis tahes muu lisateabega, kui see on kättesaadav ja asjakohane, lisades täiendavad dokumendid standardvormile ühe või mitme lisana.

2.5. Makseteenuse pakkujad peaksid järeltoiminguna vastama päritoluliikmesriigi pädevalt asutuselt saabunud lisateabe või selgituste taotlustele varem esitatud dokumentide kohta.

2.6. Makseteenuse pakkujad peaksid pidevalt hoidma päritoluliikmesriigi pädeva asutusega vahetatud teabe konfidentsiaalsust ja terviklust ning autentima end nõuetekohaselt päritoluliikmesriigi pädevale asutusele.

Esialgne aruanne

2.7. Makseteenuse pakkujad peaksid olulise operatsiooniriski- või turvaintsidendi avastamisel esitama päritoluliikmesriigi pädevale asutusele esialgse aruande.

2.8. Makseteenuse pakkujad peaksid saatma esialgse aruande pädevale asutusele 4 tunni jooksul pärast olulise operatsiooniriski- või turvaintsidendi avastamist, või kui pädeva asutuse teavituskanalid ei ole sel ajal kättesaadavad või ei toimi, tuleb aruanne esitada kohe, kui kanalid on jälle kättesaadavad/toimivad.

2.9. 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, tuleb aruanne esitada kohe, kui kanalid on jälle kättesaadavad/toimivad.

2.10. Makseteenuse pakkujad peaksid esialgsetes aruannetes esitama põhiteabe (st vormi A osa), märkides intsidendi põhitunnused ja eeldatavad tagajärjed, lähtudes intsidendi avastamise hetkel või ümberliigitamisel kättesaadavast teabest. Makseteenuse pakkujad peaksid kasutama hinnangulisi andmeid, kui tegelik teave ei ole kättesaadav. Ühtlasi peaksid makseteenuse pakkujad esialgsesse aruandes esitama järgmise uuenduse kuupäeva, mis peaks toimuma niipea kui võimalik ja kuni 3 tööpäeva jooksul.

Vahearuanne

2.11. Makseteenuse pakkujad peaksid esitama vahearuanded iga kord, kui nende hinnangul staatus oluliselt muutub, hiljemalt eelmises aruandes (esialgses aruandes või eelmises vahearuandes) märgitud järgmise uuenduse kuupäevaks.

2.12. Makseteenuse pakkujad peaksid esimese vahearuande esitamisel pädevale asutusele esitama intsidendi ja selle tagajärgede täpsema kirjelduse (vormi B osa). Lisaks peaksid makseteenuse pakkujad koostama täiendavaid vahearuandeid, uuendades vormi A ja B osas varem esitatud teavet vähemalt siis, kui nad on pärast eelmise teate esitamist saanud olulist teavet või on toimunud olulised muutused (nt kas intsident on eskaleerunud või on olukord rahunenud, kas on tuvastatud uusi põhjusi või on probleemi lahendamiseks võetud uusi meetmeid). Igal juhul peaksid makseteenuse pakkujad esitama vahearuande, kui seda nõuab päritoluliikmesriigi pädev asutus.

2.13. Sarnaselt esialgsete aruannetega peaksid makseteenuse pakkujad tegeliku teabe puudumisel kasutama hinnangulisi andmeid.

2.14. Ühtlasi peaksid makseteenuse pakkujad märkima igas aruandes järgmise uuendamise kuupäeva, mis peaks toimuma niipea kui võimalik ja kuni 3 tööpäeva jooksul. Kui makseteenuse pakkuja ei suuda esitada uuendust eeldatavaks kuupäevaks, peab ta pöörduma pädeva asutuse poole, et selgitada viivituse põhjusi, pakkuma uue võimaliku esitamise tähtaja (mitte hiljem kui 3 tööpäeva) ning saatma uue vahearuande, kus on uuendatud üksnes järgmise uuenduse hinnangulise kuupäeva teave.

2.15. Makseteenuse pakkujad peaksid saatma viimase 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 sätestatud välises teenustaseme kokkuleppes (SLA) töötlemisaegade, võimekuse, turvanõuete jne kohta, ning eriolukorra meetmed ei ole enam kasutusel.

2.16. Kui normaalne tegevus taastub 4 tunni jooksul pärast intsidendi avastamist, peaksid makseteenuse pakkujad võtma eesmärgiks esitada korraga esialgse ja vahearuande (st täitma vormi A ja B osa) 4-tunnise tähtaja jooksul.

Lõpparuanne

2.17. Makseteenuse pakkujad peaksid saatma lõpparuande pärast juurpõhjuste analüüsimist (olenemata sellest, kas leevendusmeetmed on juba rakendatud või kas lõplik juurpõhjus on tuvastatud) ning hinnangulised väärtused saab asendada tegelikega.

2.18. Makseteenuse pakkujad peaksid esitama lõpparuande pädevale asutusele kuni 2 nädala jooksul pärast normaalse äritegevuse taastumist. Kui makseteenuse pakkujad vajavad selle tähtaja pikendamist (nt kui mõju tegelikud arvandmed ei ole veel kättesaadavad), 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 avastamist, peaksid nad võtma eesmärgiks esialgses aruandes esitada esialgse, vahe- ja lõpparuande teabe.

2.20. Makseteenuse pakkujad peaksid lõpparuandes võtma eesmärgiks esitada täielik teave: 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 kokkuvõte.

2.21. Lisaks peaksid makseteenuse pakkujad saatma lõpparuande, kui intsidendi pideval hindamisel tuvastatakse, et juba teavitatud intsident ei vasta enam kriteeriumidele, mille alusel saaks seda liigitada oluliseks, ning eeldatavalt ei vasta intsident nendele kriteeriumidele ka enne lahendamist. Sellisel juhul peaksid makseteenuse pakkujad saatma lõpparuande kohe, kui see olukord tuvastatakse, ning igal juhul järgmise aruande esitamise eeldatavaks kuupäevaks. Sellisel juhul peaksid makseteenuse pakkujad vormi C osa täitmise asemel tähistama märkeruudu „Intsident liigitub muuks kui oluliseks“ ning põhjendama intsidendi taseme langetamist.

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 tagama järgmiste tingimuste täitmise:

a. Vastutuse jagunemine kõigi poolte vahel määratletakse selgesti ametlikus lepingus või (kui kohaldatav) konsolideerimisgrupi sisekorras, mille alusel toimub makseteenuse pakkuja ja kolmanda isiku vaheline delegeeritud aruandlus. Eelkõige sätestatakse selles, et sõltumata aruandluskohustuste võimalikust delegeerimisest on mõjutatud makseteenuse pakkuja täielikult vastutav ja aruandekohustuslik direktiivi (EL) 2015/2366 artiklis 96 sätestatud nõuete täitmise eest ja päritoluliikmesriigi pädevale asutusele esitatava teabe sisu eest.

b. Delegeerimine vastab oluliste tööülesannete edasi andmise nõuetele, nagu on sätestatud

   i. direktiivi (EL) 2015/2366 artikli 19 lõikes 6 seoses makseasutuste ja e-raha asutustega, mida kohaldatakse *mutatis mutandis* vastavalt direktiivi 2009/110/EÜ artiklile 3, või

   ii. Euroopa Pangandusjärelevalve Komitee krediidiasutustega seotud tegevuse edasiandmise suunistes.

c. Teave esitatakse varakult päritoluliikmesriigi pädevale asutusele ning igal juhul järgides pädeva asutuse kehtestatud tähtaegu ja protseduure, kui see on kohaldatav.

d. Pädevale asutusele esitatavate tundlike andmete konfidentsiaalsus ja 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 seesama oluline operatsiooniriski- või turvaintsident), peaksid teavitama päritoluliikmesriigi pädevat asutust, märkima kontaktandmed vormil „Mõjutatud makseteenuse pakkuja“ alla ning veenduma, et täidetud oleksid järgmised tingimused:

a. See säte peab olema lisatud delegeeritud aruandluse aluslepingusse.

b. Konsolideeritud aruandluse eeltingimuseks on juhtumid, mis on tingitud kolmanda isiku pakutavate teenuste häiretest.

c. Konsolideeritud aruandlus peab piirduma samas liikmesriigis tegutsevate makseteenuse pakkujatega.

d. Tuleb veenduda, et kolmas isik hindab intsidendi olulisust iga mõjutatud makseteenuse pakkuja jaoks ning märgib konsolideeritud aruandesse ainult need makseteenuse pakkujad, kelle jaoks liigitub intsident oluliseks. Samuti tuleb tagada, et ebakindluse korral märgitakse makseteenuse pakkuja konsolideeritud aruandesse, kui ei ole tõendatud vastupidist.

e. Kui vormil on välju, kus ei saa esitada ühist vastust (nt 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 vahemikke (väljadel, kus nii saab), mis tähistavad makseteenuse eri pakkujatel esinenud või hinnangulisi vähimaid ja suurimaid väärtusi.

f. Makseteenuse pakkujad peaksid tagama, et kolmas isik hoiab neid pidevalt kursis kogu intsidendi olulise teabega ning võimaliku kolmanda isiku ja pädeva asutuse vahelise suhtluse ja selle sisuga, kuid ainult sedavõrd, mis välistaks teiste makseteenuse pakkujate teabe korral konfidentsiaalsuse võimaliku rikkumise.

3.3. Makseteenuse pakkujad ei tohiks delegeerida oma aruandluskohustusi enne päritoluliikmesriigi pädeva asutuse teavitamist või pärast teate saamist, et edasiandmisleping ei vasta suunise 3.1 punktis b viidatud nõuetele.

3.4. Kui makseteenuse pakkujad soovivad tühistada aruandluskohustuste delegeerimise, tuleks see otsus teatada päritoluliikmesriigi pädevale asutusele vastavalt selle 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 oluliselt täitma oma aruandluskohustusi ilma välist abi kasutamata, kui kolmas isik ei teata päritoluliikmesriigi pädevale asutusele olulisest operatsiooniriski- ja turvaintsidendist vastavalt direktiivi (EL) 2015/2366 artiklile 96 ja käesolevatele suunistele. Lisaks peaksid makseteenuse pakkujad tagama, et intsidendi kohta ei esitataks aruannet kaks korda – makseteenuse pakkuja ise ja kolmas isik uuesti.

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 intsidendist 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 suhtes, lähtudes iseenda eksperdiarvamusest ning kasutades intsidendi olulisuse põhinäitajatena järgmisi kriteeriume:

a. Intsidendi põhjused kuuluvad riigi muu ametiasutuse reguleerimispädevusse (pädevusvaldkonda).
b. Intsidendi tagajärjed mõjutavad riigi muu ametiasutuse eesmärke (nt finantsstabiilsuse kaitset).
c. Intsident mõjutab või võib laialdaselt mõjutada makseteenuse pakkujaid.
d. Intsident saab tõenäoliselt või on saanud ulatuslikku meediakajastust.

5.2. Päritoluliikmesriigi pädevad asutused peaksid intsidendi kestuse ajal seda pidevalt hindama, et tuvastada muutusi, mis võiksid muuta varem asjakohatuks peetud intsidendi asjakohaseks.

6. suunis. Jagatav teave

6.1. Vaatamata muule õiguslikule alusele intsidendi teabe jagamiseks riigi muude ametiasutustega peaksid pädevad asutused esitama vastavalt suunises 5.1 märgitud riigisisestele ametiasutustele (riigi muudele asjakohastele ametiasutustele) oluliste operatsiooniriski- või turvaintsidentide teavet vähemalt esialgse aruande (või aruande, milles ajendati teavet jagama) kättesaamise ajal ning siis, kui neid teavitatakse normaalse äritegevuse taastumisest (viimase vahearuande esitamisel).

6.2. Pädevad asutused peaksid esitama riigi muudele 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 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 muude 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 muudele asjakohastele ametiasutustele aruande esitanud makseteenuse pakkuja nime ja aadressi, kui need riigi ametiasutused tagavad, et teavet käsitletakse konfidentsiaalselt.

6.4. Pädevad asutused peaksid alati säilitama salvestatud ja riigi muude asjakohaste ametiasutustega jagatud teabe konfidentsiaalsuse ja tervikluse ning autentima end nõuetekohaselt riigi muude asjakohaste ametiasutuste jaoks. Pädevad asutused peaksid eelkõige käsitlema 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 EBAga ja EKPga jagatavate intsidendiaruannete üksikasjade asjakohasuse hindamise kriteeriumide ning nende 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 (st esialgsed, vahe- ja lõpparuanded).

8. suunis. Teabevahetus

8.1. Pädevad asutused peaksid igal ajal 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 käsitlema 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 operatsioonide katkestustega seotud ohtude minimeerimiseks peaksid pädevad asutused toetama asjakohaseid teabevahetuse vahendeid.

1. lisa. Aruandlusvormid makseteenuse pakkujatele

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**

VORMIDE TÄITMISE JUHEND

Makseteenuse pakkujad peaksid täitma vormi asjakohase osa sõltuvalt aruandlusetapist: esialgse aruande jaoks A osa, vahearuannete jaoks B osa ja lõpparuande jaoks C osa. Kõik väljad on kohustuslikud, kui ei ole selgesti märgitud muud.

Pealkiri

Esialgne aruanne: esimene teade, mille makseteenuse pakkuja esitab päritoluliikmesriigi pädevale asutusele.
Vahearuanne: sama intsidendi eelmise aruande (esialgse või vahearuande) uuendus.
Viimane vahearuanne: teatab päritoluliikmesriigi pädevale asutusele, et olukord on taastunud ning äritegevus toimub normaalselt, mistõttu ei esitata rohkem vahearuandeid.
Lõpparuanne: viimane aruanne, mille makseteenuse pakkuja saadab intsidendi kohta, sest i) juurpõhjuse analüüs on valmis ja hinnangulised väärtused saab asendada tegelikega või ii) intsidenti ei peeta enam oluliseks.
Intsident liigitub muuks kui oluliseks: intsident ei vasta enam kriteeriumidele, mille alusel saab seda pidada oluliseks, ning eeldatavalt ei hakka intsident vastama nendele kriteeriumidele enne lahendamist. Makseteenuse pakkujad peaksid selgitama intsidendi taseme langetamist.
Aruande kuupäev ja kellaaeg: aruande pädevale asutusele esitamise täpne kuupäev ja kellaaeg.
Intsidendi identifitseerimisnumber (kui on kohaldatav) (vahe- ja lõpparuandes): esialgse aruande esitamisel pädevalt asutuselt saadud intsidendi unikaalne viitenumber, kui on kohaldatav (st kui pädev asutus on andnud viitenumbri).

A. Esialgne aruanne

A 1. Üldandmed

Aruande liik

Individuaalne: aruanne hõlmab üht makseteenuse pakkujat.
Konsolideeritud: aruanne hõlmab mitut makseteenuse pakkujat, kes kasutavad konsolideeritud aruandluse võimalust. Jaotise „Mõjutatud makseteenuse pakkuja“ väljad tuleks jätta täitmata (v.a väli „Intsidendist 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 on intsident.

Makseteenuse pakkuja nimi: aruandlusmenetluse alla kuuluva makseteenuse pakkuja täisnimi, nagu see on kantud kehtivasse ametlikku riiklikku makseteenuse pakkujate registrisse.
Makseteenuse pakkuja unikaalne identifitseerimisnumber, kui asjakohane: asjakohane unikaalne identifitseerimisnumber, millega tuvastatakse igas liikmesriigis makseteenuse pakkujat, mille makseteenuse pakkuja peab esitama, kui väli „Makseteenuse pakkuja tegevusloa number“ ei ole täidetud.
Makseteenuse pakkuja tegevusloa number: päritoluliikmesriigi antud tegevusloa number.
Konsolideerimisgrupi juhtettevõtja: 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 4 punktis 40 määratletud ettevõtjate gruppide korral märkige juhtettevõtja.
Päritoluriik: makseteenuse pakkuja registreeritud asukoha liikmesriik, või kui makseteenuse pakkujal puudub riigi õigusaktide kohaselt registreeritud asukoht, siis peakontori asukoha liikmesriik.

Intsidendist mõjutatud riik/riigid: riik või riigid, kus intsidendi mõju on materialiseerunud (nt mõjutatud on makseteenuse pakkuja mitu harukontorit eri riikides). Võib olla sama riik kui päritoluliikmesriik või mitte.

Peamine kontaktisik: intsidendist teatamise eest vastutava isiku ees- ja perekonnanimi, või kui mõjutatud makseteenuse pakkuja nimel teavitab kolmas isik, 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 äriettevõtte e-posti aadress.

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

Teine kontaktisik: teise isiku ees- ja perekonnanimi, kellega võib pädev asutus 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 äriettevõtte e-posti aadress.

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

Unikaalne identifitseerimisnumber, kui asjakohane: asjakohane unikaalne identifitseerimisnumber, millega tuvastatakse kolmanda isiku asukohariigis intsidendist teatavat üksust, mille aruandev üksus peab esitama, kui väli „Tegevusloa number“ ei ole täidetud.

Tegevusloa number, kui see on kohaldatav: kolmanda isiku tegevusloa number asukohariigis, kui see on kohaldatav.

Peamine 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 äriettevõtte e-posti aadress.

Telefon: telefoninumber, millelt saab vajaduse korral küsida täiendavaid selgitusi. See võib olla isiklik või äriettevõtte 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 äriettevõtte e-posti aadress.

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

A 2. Intsidendi avastamine ja esialgne liigitamine

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

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

Intsidendi lühi- ja üldkirjeldus: selgitage lühidalt intsidendi põhipunkte, võimalikke põhjusi, vahetut mõju jne.
Millal eeldatavalt esitatakse järgmine uuendus? Märkige järgmise uuenduse (vahe- või lõpparuande) esitamise eeldatav kuupäev ja kellaaeg.

B. Vahearuanne

B 1. Üldandmed

Intsidendi üksikasjalikum kirjeldus: kirjeldage intsidendi põhiomadusi, mis hõlmab vähemalt küsimustikus esitatud punkte (mis konkreetse probleemiga peab makseteenuse pakkuja tegelema, kuidas see algas ja arenes, võimalik seos varasema intsidendiga, tagajärjed, eriti makseteenuse kasutajatele jne).

Intsidendi alguse kuupäev ja kellaaeg: kuupäev ja kellaaeg, mil intsident algas, kui on teada.

Intsidendi staatus

Diagnostika: intsidendi omadused on just tuvastatud.
Parandamine: ründe all olevad komponendid on ümberkujundamisel.
Taastamine: taastatakse rikkega komponentide kõige viimast taastatavat olekut.
Ennistamine: maksetega seotud teenuseid osutatakse jälle.

Intsidendist taastumise või eeldatava taastumise kuupäev ja kellaaeg: märkige kuupäev ja kellaaeg, mil intsident saadi või saadakse eeldatavalt kontrolli alla ning normaalne äritegevus jätkus või eeldatavalt jätkub.

B 2. Intsidendi liigitamine / intsidendi teave

Üldmõju: märkige, mis valdkondi intsident mõjutas. Valida võib mitu vastusevarianti.

Terviklus: varade (sh andmete) täpsus ja terviklus on kaitstud.
Käideldavus: maksetega seotud teenused on makseteenuse kasutajatele kättesaadavad ja kasutatavad.
Konfidentsiaalsus: teavet ei tehta kättesaadavaks ega avalikustata volitamata isikutele, üksustele ega protsessidele.
Autentsus: allikas on sama, mis see väidab end olevat.
Talitluspidevus: organisatsiooni protsessid, toimingud ja varad, mida on vaja maksetega seotud teenuste osutamiseks, on täielikult juurdepääsetavad ning toimivad heakskiidetud eelmääratletud tasemetel.

Mõjutatud tehingud: makseteenuse pakkujad peaksid märkima, mis piirmäärad intsident saavutas või tõenäoliselt saavutab, ja seonduvad väärtused: mõjutatud tehingute arv, mõjutatud tehingute protsent intsidendist mõjutatud samade makseteenuste kaudu sooritatud maksetehingute arvust ning tehingute koguväärtus. Makseteenuse pakkujad peaksid esitama nende muutujate kohta konkreetsed väärtused, mis võivad olla tegelikud arvud või hinnangud. Mitme makseteenuse pakkuja nimel intsidendist teatavad üksused (st konsolideeritud aruandluse korral) võivad selle asemel esitada aruandes sisalduvas mitmest makseteenuse pakkujast koosnevas grupis täheldatud või hinnangulised väärtuste vahemikud, mis tähistavad vähimaid ja suurimaid väärtusi, ning eraldada need sidekriipsuga. 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 makseteatise sisu muudeti ja mis telliti pettuse teel (olenemata sellest, kas vahendid on tagasi saadud või mitte). Lisaks peaksid makseteenuse pakkujad arvestama maksetehingute tavatasemena aasta keskmist taset igapäevaste riigisiseste ja piiriüleste maksetehingute korral, mis on sooritatud koos samade makseteenustega, mida

intsident mõjutas, võttes arvutuste võrdlusperioodiks eelmise aasta. Kui makseteenuse pakkujad ei pea seda suurust tüüpiliseks (nt hooajalisuse tõttu), tuleb kasutada muud iseloomulikumat suurust ning esitada pädevale asutusele meetodi aluseks olevad põhjendused vormi väljal „Märkused“.

Mõjutatud makseteenuse kasutajad: makseteenuse pakkujad peaksid märkima, mis piirmäärad intsident saavutas või tõenäoliselt saavutab, ja seonduvad väärtused: mõjutatud makseteenuse kasutajate koguarv ning mõjutatud makseteenuse kasutajate protsent makseteenuse kasutajate koguarvust. Makseteenuse pakkujad peaksid esitama nende muutujate kohta konkreetsed väärtused, mis võivad olla tegelikud arvud või hinnangud. Mitme makseteenuse pakkuja nimel intsidendist teatavad üksused (st konsolideeritud aruandluse korral) võivad selle asemel esitada aruandes sisalduvas mitmest makseteenuse pakkujast koosnevas grupis täheldatud või hinnangulised väärtuste vahemikud, mis tähistavad vähimaid ja suurimaid väärtusi, ning eraldada need sidekriipsuga. 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 määrama makseteenuse nende kasutajate arvu, kes võisid kasutada makseteenust intsidendi kestuse ajal. Konsolideerimisgruppide korral peaks iga makseteenuse pakkuja arvestama ainult enda makseteenuse kasutajaid. Kui makseteenuse pakkuja osutab tegevusega seotud teenuseid teistele makseteenuse pakkujatele, peaks ta arvestama ainult enda makseteenuse kasutajaid (kui need on olemas), ning neid tegevusega seotud teenuseid kasutavad makseteenuse pakkujad peaksid hindama intsidenti enda makseteenuse kasutajate suhtes. Lisaks peaksid makseteenuse pakkujad pidama 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).

Teenuse seisuaeg: makseteenuse pakkujad peaksid märkima, kas intsident on saavutanud või tõenäoliselt saavutab teatud piirmäära, ja seonduva väärtuse: teenuse kogu seisuaeg. Makseteenuse pakkujad peaksid esitama selle muutuja kohta konkreetsed väärtused, mis võivad olla tegelikud arvud või hinnangud. Mitme makseteenuse pakkuja nimel intsidendist teatavad üksused (st konsolideeritud aruandluse korral) võivad selle asemel esitada aruandes sisalduvas mitmest makseteenuse pakkujast koosnevas grupis täheldatud või hinnangulised väärtuste vahemikud, mis tähistavad vähimaid ja suurimaid väärtusi, ning eraldada need sidekriipsuga. 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 äritegevuseks (vajalik makseteenuste teostamiseks), kui ka ajavahemikke, mil nad on suletud, ning hooldusperioode, kui need on asjakohased ja kohaldatavad. Kui makseteenuse pakkujad ei suuda määrata teenuse seisuaja algust, peaksid nad erandkorras arvestama teenuse seisuaega alates selle avastamisest.

Majandusmõju: makseteenuse pakkujad peaksid märkima, kas intsident on saavutanud või tõenäoliselt saavutab teatud piirmäära, ja seonduvad väärtused: otsesed ja kaudsed kulud. Makseteenuse pakkujad peaksid esitama nende muutujate kohta konkreetsed väärtused, mis võivad olla tegelikud arvud või hinnangud. Mitme makseteenuse pakkuja nimel intsidendist teatavad üksused (st konsolideeritud aruandluse korral) võivad selle asemel esitada aruandes

sisalduvas mitmest makseteenuse pakkujast koosnevas grupis täheldatud või hinnangulised väärtuste vahemikud, mis tähistavad vähimaid ja suurimaid väärtusi, ning eraldada need sidekriipsuga. 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.

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

Kaudsed kulud: rahasumma (eurodes), mis kaasnes intsidendiga kaudse kuluna (nt kliendile kahju hüvitamise / hüvitiste kulud, ärivõimaluste puudumise tagajärjel kaotatud tulu, võimalikud õiguskulud).

Suur ettevõttesisene eskalatsioon: makseteenuse pakkujad peaksid kaalutlema, kas seoses intsidendi mõjuga makseteenustele on intsidendist teavitatud või tuleks tõenäoliselt teavitada IT-juhti (või sarnasel ametikohal olevat isikut) väljaspool korralise teavitamise korda ning pidevalt kogu intsidendi kestuse ajal. Delegeeritud aruandluse korral toimub eskalatsioon kolmanda isiku siseselt. 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 finantsturule, mida mõistetakse finantsturu taristutena ja/või maksekaardiskeemidena, mis toetavad seda ja teisi makseteenuse pakkujaid. Makseteenuse pakkujad peaksid eelkõige hindama, kas intsident kordus või tõenäoliselt kordub teiste makseteenuse pakkujate korral, kas see on mõjutanud või tõenäoliselt mõjutab finantsturu taristute sujuvat toimimist ning kas see ohustas või tõenäoliselt ohustab finantssüsteemi stabiilsust 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.

Mõju mainele: makseteenuse pakkujad peaksid arvestama nähtavuse ulatust, mille intsident on nende parima teadmise kohaselt turul saavutanud 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) intsident on mõjutanud nähtavat protsessi ning seda võidakse kajastada või seda on juba kajastatud meedias (peale tavapärase meedia, nt ajalehtede, ka blogides, suhtlusvõrgustikes jne); ii) õigusaktidest tulenevad kohustused on jäetud täitmata või jäetakse tõenäoliselt täitmata; iii) rikkumiste eest on kohaldatud või tõenäoliselt kohaldatakse sanktsioone või iv) sarnane intsident on toimunud ka varem.

B 3. Intsidendi kirjeldus

Intsidendi liik: märkige, kas teile teadaolevalt on intsident operatsiooniriski- või turvaintsident.

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

Turvaintsident: makseteenuse pakkuja varadele volitamata juurdepääs, nende kasutamine, avalikustamine, katkestamine, muutmine või hävitamine, mis mõjutab

makseteenuste terviklust, käideldavust, konfidentsiaalsust, autentsust ja/või talitluspidevust. See võib toimuda muu hulgas makseteenuse pakkujal esinevate küberrünnakute, puudulikult väljatöötatud või rakendatud turvameetmete või ebapiisava füüsilise julgeoleku korral.

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

Põhjust uuritakse: põhjust ei ole veel leitud.

Välisrünne: põhjuse allikas tuleb väljastpoolt ning on tahtlikult suunatud makseteenuse pakkujale (nt pahavara ründed).

Siserünne: põhjuse allikas tuleb seestpoolt ning on tahtlikult suunatud makseteenuse pakkujale (nt sisepettus).

Ründe liik

Hajus-/ummistusrünne (D/DoS): katse muuta veebiteenus kättesaamatuks, koormates selle üle eri allikatest pärit võrguliiklusega.

Sisesüsteemide nakatamine: kahjulik tegevus, millega rünnatakse arvutisüsteeme, proovides varastada kõvakettaruumi või protsessoriaega, saada juurdepääsu privaatsetele andmetele, rikkuda andmeterviklust, saata kontaktidele rämpsposti jne.

Sihipärane sissetung: volitamata tegevus, näiteks salajane jälgimine, nuhkimine ja teabe varastamine küberruumi kaudu.

Muu: muud liiki rünne, mille all makseteenuse pakkuja võis kannatada otseselt või teenusepakkuja kaudu. See variant tuleb valida eelkõige siis, kui rünne on toimunud autoriseerimis- ja autentimisprotsessi vastu. Üksikasjad tuleb märkida vabatekstiväljale.

Välissündmused: põhjus on seotud sündmustega, mille üle puudub organisatsioonil üldiselt voli (nt loodusõnnetused, õigusküsimused, äriküsimused ning teenustest sõltumine).

Inimlik eksimus: intsidendi põhjustas tahtmatu inimlik eksimus, kas maksemenetluse osana (nt vale maksete pakkfaili üleslaadimine maksesüsteemi) või sellega mingil viisil seoses (nt tahtmatu elektrikatkestuse tõttu pannakse maksetoiming ootele).

Protsessi rike: intsidendi põhjustas puudulikult väljatöötatud või rakendatud makseprotsess, protsessi juhttoimingud ja/või tugiprotsessid (nt muutmis-/migratsiooni-, katsetamis-, konfigureerimis-, suutlikkuse tagamise, jälgimisprotsess).

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

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

Kas intsident mõjutas teid otseselt või kaudselt teenusepakkuja kaudu? Intsident võib mõjutada makseteenuse pakkujat otseselt või kaudselt kolmanda isiku kaudu. Kaudse mõju korral märkige teenusepakkuja(te) nimi (nimed).

B 4. Intsidendi mõju

Mõjutatud hoone(d) (aadress), kui on kohaldatav: kui mõjutatud on füüsiline hoone, märkige selle aadress.

Mõjutatud kommertskanalid: märkige makseteenuse kasutajatega suhtlemiseks kasutav 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 äritegevusele omaseid tehinguid. Kõiki tegutsemiskohti, mille ühes liikmesriigis on asutanud teises liikmesriigis oleva 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.

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

Müügikoht: kaupleja füüsiline tegevuskoht, kus maksetehing algatatakse.

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

Mõjutatud makseteenused: märkige makseteenused, mis ei tööta 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 ning 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.

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

Otsekorraldused: makseteenus, millega debiteeritakse maksja maksekontot, millelt makse saaja on alustanud maksetehingut, maksja poolt makse saajale, makse saaja makseteenuse pakkujale või maksja enda makseteenuse pakkujale antud nõusoleku kohaselt.

Kaardimaksed: maksekaardiskeemi taristul ja ärieeskirjadel põhinev makseteenus maksetehingu tegemiseks kaardiga, sidevahendiga, digitaalse või IT-seadme või tarkvaraga, kui selle tulemuseks on deebet- või kreeditkaarditehing. 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 makseinstrumendi maksja maksetehingute algatamiseks ja töötlemiseks.

Rahasiire: makseteenus, mille kaudu saadakse maksjalt rahalisi vahendeid ilma maksja või makse saaja nimel maksekontosid loomata, mille eesmärk on vastava summa ülekandmine makse saajale või makse saaja nimel tegutsevale teisele 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 asuva maksekonto suhtes.

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

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

Mõjutatud funktsionaalsed valdkonnad: märkige intsidendist mõjutatud makseprotsessi etapp või etapid. Valida võib mitu vastusevarianti.

Autentimine/autoriseerimine: menetlused, mille kaudu makseteenuse pakkuja saab tuvastada makseteenuse kasutaja isiku või konkreetse maksevahendi kasutamise kehtivust, sh kasutaja isikustatud turvavolitusi ja makseteenuse kasutajat (või selle kasutaja nimel tegutsevat kolmandat isikut), kes annab oma nõusoleku vahendite või väärtpaberite ülekandmiseks.

Side: 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 kohustusi vahendite ülekandmise kaudu, kui toimingut sooritab mõjutatud makseteenuse pakkuja ise.

Kaudne arveldus: tehingu või töötlemise lõpuleviimine eesmärgiga täita osalejate kohustusi vahendite ülekandmise kaudu, kui toimingut sooritab mõjutatud makseteenuse pakkuja nimel teine makseteenuse pakkuja.

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

Mõjutatud süsteemid ja komponendid: märkige makseteenuse pakkuja tehnoloogilise taristu osa või osad, mida on intsident mõjutanud. Valida võib mitu vastusevarianti.

Rakendus/tarkvara: programmid, operatsioonisüsteemid jne, mis toetavad makseteenuse pakkuja makseteenuste osutamist.

Andmebaas: andmestruktuur, mis säilitab maksetehingute teostamiseks vajalikke isiku- ja makseandmeid.

Riistvara: füüsilised tehnikaseadmed, mille abil käitatakse protsesse ja/või säilitatakse andmeid, mida makseteenuse pakkujad vajavad maksetega seotud toimingute sooritamiseks.

Võrk/taristu: sidevõrgud (avalikud või eravõrgud), mis võimaldavad makseprotsessi ajal andme- ja teabevahetust (nt internet).

Muu: mõjutatud süsteem ja komponent on muu kui loetletud eespool. Täiendavad üksikasjad tuleb märkida vabatekstiväljale.

Mõjutatud töötajad: märkige, kas intsident on mõjutanud makseteenuse pakkuja töötajaid või mitte; kui on, märkige täiendavad üksikasjad vabatekstiväljale.

B 5. Intsidendi mõju leevendamine

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

Kas talitluspidevuse ja/või taasteplaanid on käivitatud? Märkige „jah“ või „ei“; kui jah, märkige juhtunu põhiandmed (millal kavad käivitati ja mida need sisaldavad).
Kas makseteenuse pakkuja on intsidendi tõttu tühistanud või nõrgendanud teatud kontrolle? Märkige, kas makseteenuse pakkuja on pidanud intsidendi lahendamisel teatud kontrolle eirama (nt lõpetanud nn nelja silma põhimõtte kasutamise); kui jah, põhjendage kontrollide nõrgendamist või tühistamist.

C. Lõpparuanne

C 1. Üldandmed

Vahearuande teabe uuendus (kokkuvõte): esitage intsidendist taastumiseks ja selle kordumise vältimiseks rakendatud meetmete lisateave, juurpõhjuse analüüs, saadud kogemused jne.

Intsidendi sulgemise kuupäev ja kellaaeg: märkige kuupäev ja kellaaeg, mil intsidendi staatus loeti suletuks.

Kas algsed kontrollid on jälle kasutusel? Kui makseteenuse pakkuja pidi intsidendi tõttu tühistama või nõrgendama teatud kontrolle, märkige, kas need kontrollid on jälle kasutusel, ning esitage lisateave vabatekstiväljal.

C 2. Juurpõhjuse analüüs ja järeltoimingud

Mis oli juurpõhjus, kui see on juba teada? Selgitage, mis oli intsidendi juurpõhjus, või kui see ei ole veel teada, siis juurpõhjuse analüüsi põhjal tehtud esialgsed järeldused. Makseteenuse pakkuja võib vajaduse korral lisada üksikasjaliku teabega faili.

Peamised rakendatud parandusmeetmed või kavandatavad meetmed intsidendi kordumise takistamiseks tulevikus, kui on juba teada: kirjeldage peamisi meetmeid, mida on rakendatud või kavatsetakse rakendada, et takistada intsidendi kordumist 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 intsidendist 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).