EBA/GL/2017/10

19/12/2017

Riktlinjer

för rapportering vid allvarliga incidenter enligt direktiv (EU) 2015/2366 (andra betaltjänstdirektivet)

1. Efterlevnads- och rapporteringsskyldigheter

Riktlinjernas status

1. Detta dokument innehåller riktlinjer som har utfärdats enligt artikel 16 i förordning (EU) nr 1093/2010[1]. I enlighet med artikel 16.3 i förordning (EU) nr 1093/2010 måste behöriga myndigheter och finansinstituten med alla tillgängliga medel försöka följa riktlinjerna.

2. Avriktlinjerframgår Europeiska bankmyndighetens (EBA) syn på lämplig tillsynspraxis inom det europeiska systemet för finansiell tillsyn eller på hur unionslagstiftningen ska tillämpas inom ett särskilt område. Behöriga myndigheter enligt definitionen i artikel 4.2 i förordning (EU) nr 1093/2010 som berörs av riktlinjerna ska följa dem genom att på lämpligt sätt införliva dem i sin praxis (till exempel genom att ändra sina rättsliga ramar eller tillsynsrutiner), även när riktlinjerna i första hand riktas till finansinstitut.

Rapporteringskrav

3. Enligt artikel 16.3 i förordning (EU) nr 1093/2010 måste de behöriga myndigheterna meddela EBA om de följer eller avser att följa dessa riktlinjer, alternativt ange skälen till att de inte gör det, senast den 19/02/2018 Om någon sådan anmälan inte inkommer inom denna tidsfrist kommer EBA att anse att de behöriga myndigheterna inte följer riktlinjerna. Anmälningar ska lämnas på det formulär som tillhandahålls på EBA:s webbplats till compliance@eba.europa.eu med hänvisningen ”EBA/GL/2017/10”. Anmälningar ska inges av personer som har befogenhet att rapportera om hur reglerna efterlevs på de behöriga myndigheternas vägnar. Alla förändringar i graden av efterlevnad måste rapporteras till EBA.

4. Anmälningarna kommer att offentliggöras på EBA:s webbplats i enlighet med artikel 16.3.

[1] Europaparlamentets och rådets förordning (EU) nr 1093/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska bankmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/78/EG (EUT L 331, 15.12.2010, s. 12).

2. Syfte, tillämpningsområde och definitioner

Syfte

5. Dessa riktlinjer härrör från ett bemyndigande till EBA enligt artikel 96.3 i Europaparlamentets och rådets direktiv 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden och om ändring av direktiven 2002/65/EG, 2009/110/EG, 2013/36/EG samt förordning (EU) nr 1093/2010 samt upphävande av direktiv 2007/64/EG (nedan kallat andra betaltjänstdirektivet).

6. I dessa riktlinjer specificeras särskilt kriterierna för klassificeringen av allvarliga operativa eller säkerhetsincidenter från betaltjänstleverantörer samt det format och de förfaranden som föreskrivs i artikel 96.1 i ovannämnda direktiv som de ska följa för att anmäla sådana incidenter till den behöriga myndigheten i hemmedlemsstaten.

7. I dessa riktlinjer behandlas dessutom det sätt på vilket dessa behöriga myndigheter ska bedöma incidentens relevans samt vilka uppgifter i incidentrapporterna andra nationella myndigheter enligt artikel 96.2 i nämnda direktiv ska få ta del av.

8. I dessa riktlinjer behandlas även vilka relevanta uppgifter om de rapporterade incidenterna som EBA och ECB ska få ta del av i syfte att främja en gemensam och enhetlig strategi.

Tillämpningsområde

9. Dessa riktlinjer är tillämpliga med avseende på klassificeringen och rapporteringen av allvarliga operativa eller säkerhetsincidenter i enlighet med artikel 96 i direktiv (EU) 2015/2366.

10. Dessa riktlinjer är tillämpliga på samtliga incidenter som omfattas av definitionen ”allvarliga operativa eller säkerhetsincidenter”, vilket omfattar både externa och interna händelser som antingen kan utgöra uppsåtliga handlingar eller olyckshändelser.

11. Dessa riktlinjer är även tillämpliga när den allvarliga operativa eller säkerhetsincidenten har sitt ursprung utanför unionen (t.ex. när en incident har sitt ursprung i moderbolaget eller i ett dotterbolag som är etablerat utanför unionen) och påverkar de betaltjänster som en betaltjänstleverantör som är etablerad i unionen antingen tillhandahåller direkt (ett drabbat bolag som är etablerat utanför unionen utför en betalningsrelaterad tjänst) eller indirekt (betaltjänstleverantörens fortsatta betalningsverksamhet äventyras på annat sätt till följd av incidenten).

Adressater

12. Den första uppsättningen riktlinjer (avsnitt 4) riktar sig till betaltjänstleverantörer såsom de definieras i artikel 4.11 i direktiv (EU) 2015/2366 och såsom anges i artikel 4.1 i förordning (EU) nr 1093/2010.

13. Den andra och tredje uppsättningen riktlinjer (avsnitt 5 and 6) riktar sig till behöriga myndigheter såsom de definieras i artikel 4.2 i) i förordning (EU) nr 1093/2010.

Definitioner

14. Om inte annat anges har de termer som används och definieras i direktiv (EU) 2015/2366 samma betydelse i riktlinjerna. Dessutom gäller följande definitioner i dessa riktlinjer:

Operativa eller säkerhetsincidenter	En enskild händelse eller en serie av sammanhängande händelser som inte har planerats av betaltjänstleverantören vilka har eller sannolikt kommer att få negativa effekter på betalningsrelaterade tjänster vad gäller integritet, tillgänglighet, konfidentialitet, autenticitet och/eller kontinuitet.
Integritet	Innebär ett säkerställande av att tillgångarna (inbegripet data) är korrekta och fullständiga.
Tillgänglighet	Innebär att betalningsrelaterade tjänster är tillgängliga och kan användas av betaltjänstanvändarna.
Konfidentialitet	Innebär att information inte görs tillgänglig eller lämnas ut till icke auktoriserade personer, enheter eller förfaranden.
Autenticitet	Innebär att en källa är vad den utger sig för att vara.
Kontinuitet	Innebär att de processer, uppgifter och tillgångar som en organisation behöver för att leverera betalningsrelaterade tjänster är fullt tillgängliga och fungerar på i förväg fastställda godtagbara nivåer.
Betalningsrelaterade tjänster	All affärsverksamhet i den mening som avses i artikel 4.3 i andra betaltjänstdirektivet och all teknisk support som behövs för ett korrekt tillhandahållande av betaltjänster.

3. Genomförande

Datum för tillämpning

15. Dessa riktlinjer gäller från den 13 januari 2018.

4. Riktlinjer som vänder sig till betaltjänstleverantörer avseende anmälan av allvarliga operativa eller säkerhetsincidenter till den behöriga myndigheten i deras hemmedlemsstat

Riktlinje 1: Klassificering som en allvarlig incident

1.1. Betaltjänstleverantörer ska klassificera operativa eller säkerhetsincidenter som allvarliga när de uppfyller

a. ett eller flera av kriterierna för den ” högre effektnivån”, eller

b. tre eller flera av kriterierna för den ”lägre effektnivån”

såsom föreskrivs i punkt 1.4 i riktlinjerna och i enlighet med den bedömning som fastställs i dessa riktlinjer.

1.2. Betaltjänstleverantörer ska bedöma en operativ incident eller en säkerhetsincident mot bakgrund av följande kriterier och deras underliggande indikatorer:

i. Berörda transaktioner

Betaltjänstleverantörer ska fastställa det totala värdet av de transaktioner som påverkas samt antalet betalningar som äventyrats som en procentandel av de vanliga betalningstransaktioner som utförs genom de berörda betaltjänsterna.

ii. Berörda betaltjänstanvändare

Betaltjänstleverantörer ska fastställa antalet berörda betaltjänstanvändare både i absoluta siffror och som en procentandel av det totala antalet betaltjänstanvändare.

iii. Driftavbrott

Betaltjänstleverantörer ska fastställa under hur lång tid tjänsten sannolikt inte kommer att vara tillgänglig för betaltjänstanvändarna eller när betalningsordern, i den mening som avses i artikel 4.13 i andra betaltjänstdirektivet, inte kan fullgöras av betaltjänstleverantören.

iv. Ekonomiska effekter

Betaltjänstleverantörer ska fastställa vilka sammanlagda kostnader incidenten medför och beakta både den absoluta siffran och, i förekommande fall, den relativa betydelse dessa kostnader har i förhållande till betaltjänstleverantörens storlek (dvs. till betaltjänstleverantörens primärkapital).

v. Hög intern upptrappningsnivå

Betaltjänstleverantörer ska bedöma huruvida incidenten har rapporterats eller sannolikt kommer att rapporteras till deras verkställande ledning.

vi. Andra betaltjänstleverantörer eller relevanta infrastrukturer som kan beröras

Betaltjänstleverantörer ska fastställa vilka systemrelaterade effekter incidenten sannolikt kommer att få, dvs. huruvida den eventuellt kan sprida sig från den ursprungligen berörda betaltjänstleverantören till andra betaltjänstleverantörer, infrastrukturer på den finansiella marknaden och/eller system för kortbetalning.

vii. Effekter på anseendet

Betaltjänstleverantörer ska fastställa hur incidenten kan undergräva användarnas förtroende för betaltjänstleverantören själv och, mer allmänt, för den underliggande tjänsten eller marknaden i dess helhet.

1.3. Betaltjänstleverantörer ska beräkna indikatorernas värde enligt följande metod:

i. Berörda transaktioner

I allmänhet bör betaltjänstleverantörer tolka ”berörda transaktioner” som alla inhemska och gränsöverskridande transaktioner som direkt eller indirekt har påverkats eller sannolikt kommer att påverkas av incidenten och, i synnerhet, transaktioner som inte kunde initieras eller behandlas, transaktioner där innehållet i betalningsmeddelandet ändrats och transaktioner som beställts i bedrägligt syfte (oberoende av huruvida medlen har återvunnits eller inte).

Vidare ska betaltjänstleverantörer tolka den normala nivån av betalningstransaktioner som det dagliga årliga genomsnittet av inhemska och gränsöverskridande betalningstransaktioner som genomförs med samma betaltjänst som har påverkats av incidenten, med föregående år som referensperiod för beräkningarna. Om betaltjänstleverantörer inte anser att denna siffra är representativ (t.ex. på grund av säsongsvariationer), ska de använda en annan, mer representativ, parameter och informera den behöriga myndigheten om de underliggande skälen för detta tillvägagångssätt i det motsvarande fältet i mallen (se bilaga 1).

ii. Berörda betaltjänstanvändare

Betaltjänstleverantörer ska tolka ”berörda betaltjänstanvändare” som samtliga kunder (antingen inhemska eller utländska, konsumenter eller företag) som har ett avtal med den berörda betaltjänstleverantören som ger dem tillgång till den berörda betaltjänsten, och som har drabbats eller sannolikt kommer att drabbas av konsekvenserna av incidenten. Betaltjänstleverantörer ska göra uppskattningar som grundas på deras tidigare verksamhet för att fastställa det antal betaltjänstanvändare som kan ha använt betaltjänsten under den tid som incidenten pågick.

Vad gäller koncerner ska varje betaltjänstleverantör endast beakta sina egna betaltjänstanvändare. Om en betaltjänstleverantör erbjuder operativa tjänster till andra ska den betaltjänstleverantören endast beakta sina egna betaltjänstanvändare (om det föreligger sådana) och betaltjänstleverantörer som tar emot dessa operativa tjänster ska bedöma incidenten i förhållande till sina egna betaltjänstanvändare.

Vidare ska betaltjänstleverantörer tolka det totala antalet betaltjänstanvändare som det sammanlagda antalet inhemska och gränsöverskridande betaltjänstanvändare som var bundna genom avtal till dem när incidenten inträffade (eller, alternativt, de senaste tillgängliga sifferuppgifterna) och hade tillgång till den berörda betaltjänsten, oberoende av deras storlek eller huruvida de anses utgöra aktiva eller passiva betaltjänstanvändare.

iii. Driftavbrott

Betaltjänstleverantörer ska beakta den period som varje uppgift, process eller kanal med anknytning till tillhandahållandet av betaltjänster är eller sannolikt kommer att vara ur funktion och således utgör hinder för i) initiering och/eller genomförande av en betaltjänst och/eller ii) tillgång till ett betalkonto. Betaltjänstleverantörer ska räkna driftavbrottet från den tidpunkt det uppkommer och beakta såväl tidsintervaller när de är öppna för handel såsom krävs för genomförandet av betaltjänster som intervaller när de är stängda och underhållsperioder, om det är relevant och i förekommande fall. Om betaltjänstleverantörer inte kan fastställa när driftavbrottet inträffade ska de undantagsvis beräkna det från den tidpunkt när det upptäcktes.

iv. Ekonomiska effekter

Betaltjänstleverantörer ska beakta både kostnader som har en direkt anknytning till incidenten och sådana som har en indirekt anknytning till incidenten. Betaltjänstleverantörer ska bland annat beakta exproprierade medel eller tillgångar, kostnader för utbyte av maskin- eller programvara, andra juridiska kostnader eller kostnader för avhjälpande, avgifter på grund av åsidosättande av avtalsförpliktelser, sanktioner, externa skulder och förlorade intäkter. Vad gäller indirekta kostnader ska betaltjänstleverantörerna endast beakta kostnader som redan är kända eller med stor sannolikhet kommer att dyka upp.

v. *Hög intern upptrappningsnivå*

Betaltjänstleverantörer ska beakta huruvida den informationsansvariga (eller en person i liknande ställning) har informerats eller sannolikt kommer att informeras om incidenten på grund av dess påverkan på betalningsrelaterade tjänster, utöver vid ett eventuellt periodiskt anmälningsförfarande samt kontinuerligt under den tid incidenten pågick. Dessutom ska betaltjänstleverantörer beakta huruvida ett krisläge har utlösts eller sannolikt kommer att utlösas som ett resultat av incidentens påverkan på betalningsrelaterade tjänster.

vi. *Andra betaltjänstleverantörer eller relevanta infrastrukturer som kan beröras*

Betaltjänstleverantörer ska bedöma incidentens påverkan på den finansiella marknaden, vilken ska tolkas som infrastrukturer och/eller kortbetalningssystem på den finansiella marknaden som stödjer dem och andra betaltjänstleverantörer. I synnerhet ska betaltjänstleverantörer bedöma huruvida incidenten har spridit sig eller sannolikt kommer att sprida sig till andra betaltjänstleverantörer, huruvida den har påverkat eller sannolikt kommer att påverka om infrastrukturerna på den finansiella marknaden fungerar väl och huruvida den har äventyrat eller sannolikt kommer att äventyra den sunda driften av det finansiella systemet i dess helhet. Betaltjänstleverantörer ska ta hänsyn till olika parametrar såsom huruvida den berörda komponenten/programvaran är privatägd eller tillgänglig för allmänheten, huruvida det äventyrade nätverket är internt eller externt och huruvida betaltjänstleverantören har slutat fullgöra eller sannolikt kommer att sluta fullgöra sina skyldigheter i de finansiella marknadsinfrastrukturer där betaltjänstleverantören är medlem.

vii. *Effekter på anseendet*

Betaltjänstleverantörer ska beakta, såvitt de vet, hur synlig incidenten har blivit eller sannolikt kommer att bli på marknaden. I synnerhet ska betaltjänstleverantörer beakta hur sannolikt det är att incidenten kommer att skada samhället som en bra indikator på dess potentiella effekter på deras anseende. Betaltjänstleverantörer ska beakta huruvida i) incidenten har påverkat en synlig process och därför sannolikt kommer att uppmärksammas eller redan har uppmärksammats i media (inte endast med beaktande av traditionella media, såsom tidningar, utan även bloggar, sociala nätverk etc.), ii) skyldigheter enligt lag har åsidosatts eller sannolikt kommer att åsidosättas, iii) sanktioner har åsidosatts eller sannolikt kommer att åsidosättas eller iv) samma typ av incident har inträffat tidigare.

1.4. Betaltjänstleverantörer ska bedöma en incident genom att fastställa om de relevanta trösklarna i tabell 1 har överskridits eller sannolikt kommer att överskridas för varje enskilt kriterium innan incidenten har avhjälpts.

Tabell 1: Tröskelvärden

Kriterier	Lägre effektnivå	Högre effektnivå
Berörda transaktioner	> 10 % av betaltjänstleverantörens normala transaktionsnivå (vad gäller antalet transaktioner) **och** > 100 000 euro	> 25 % av betaltjänstleverantörens normala transaktionsnivå (vad gäller antalet transaktioner) **eller** > 5 miljoner euro
Berörda betaltjänstanvändare	> 5 000 **och** > 10 % av betaltjänstleverantörens betaltjänstanvändare	> 50 000 **eller** > 25 % av betaltjänstleverantörens betaltjänstanvändare
Driftavbrott	> 2 timmar	Ej tillämpligt
Ekonomiska effekter	Ej tillämpligt	> Max. (0,1 % av primärkapitalet,* 200 000 euro) **eller** > 5 miljoner euro
Hög intern upptrappningsnivå	Ja	Ja, och krisläge (eller liknande) kommer sannolikt att utlysas
Andra betaltjänstleverantörer eller relevanta infrastrukturer som kan beröras	Ja	Ej tillämpligt
Effekter på anseendet	Ja	Ej tillämpligt

*Primärkapital såsom det definieras i artikel 25 i Europaparlamentets och rådets förordning (EU) nr 575/2013 av den 26 juni 2013 om tillsynskrav för kreditinstitut och värdepappersföretag och om ändring av förordning (EU) nr 648/2012.

1.5. Betaltjänstleverantörer som inte har tillräckliga faktiska uppgifter till stöd för sin bedömning av huruvida en viss tröskel har nåtts eller sannolikt kommer att nås innan incidenten har avhjälpts ska göra en uppskattning (t.ex. under den inledande utredande fasen).

1.6. Betaltjänstleverantörer ska kontinuerligt göra en sådan bedömning under den tid incidenten pågår för att identifiera en eventuell statusförändring, antingen uppåt (från mindre allvarlig till allvarlig) eller neråt (från allvarlig till mindre allvarlig).

Riktlinje 2: Anmälningsförfarande

2.1. Betaltjänstleverantörer ska samla in all relevant information, upprätta en incidentrapport genom att använda mallen som tillhandahålls i bilaga 1 och ge in den till den behöriga myndigheten i hemmedlemsstaten. Betaltjänstleverantörer ska fylla i mallen i enlighet med de instruktioner som tillhandahålls i bilaga 1.

2.2. Betaltjänstleverantörer ska använda samma mall för att informera den behöriga myndigheten under den tid incidenten pågår (dvs. för inledande, mellanliggande och slutliga rapporter, såsom beskrivs i punkterna 2.7–2.21). Betaltjänstleverantörer ska fylla i mallen etappvis, efter bästa förmåga, när mer information blir tillgänglig allteftersom deras interna utredning framskrider.

2.3. Betaltjänstleverantörer ska även lämna en kopia av den information som har tillhandahållits (eller kommer att tillhandahållas) till deras användare till den behöriga myndigheten i deras hemmedlemsstat, om tillämpligt, såsom föreskrivs i andra stycket i artikel 96.1 i andra betaltjänstdirektivet, så snart som den är tillgänglig.

2.4. Betaltjänstleverantörer ska tillhandahålla kompletterande upplysningar till den behöriga myndigheten i hemmedlemsstaten, såvitt de är tillgängliga och bedöms vara relevanta för den behöriga myndigheten, genom att bifoga kompletterande dokument till de standardiserade mallarna som en eller flera bilagor.

2.5. Betaltjänstleverantörer ska följa upp varje begäran från den behöriga myndigheten i hemmedlemsstaten om ytterligare information eller klargöranden med avseende på den dokumentation som redan ingetts.

2.6. Betaltjänstleverantörer ska alltid säkerställa konfidentialiteten och integriteten när det gäller den information som utväxlats med den behöriga myndigheten i deras hemmedlemsstat och även autentisera sig själva på ett korrekt sätt i förhållande till den behöriga myndigheten i deras hemmedlemsstat.

Inledande rapport

2.7. Betaltjänstleverantörer ska ge in en inledande rapport till den behöriga myndigheten i hemmedlemsstaten när en allvarlig operativ incident eller säkerhetsincident först upptäcks.

2.8. Betaltjänstleverantörer ska skicka den inledande rapporten till den behöriga myndigheten inom fyra timmar efter det att den allvarliga operativa eller säkerhetsincidenten först upptäcktes, eller, vid vetskap om att den behöriga myndighetens rapporteringskanaler inte är tillgängliga eller i funktion vid denna tidpunkt, så snart som de är tillgängliga/i funktion igen.

2.9. Betaltjänstleverantörer ska även ge in en inledande rapport till den behöriga myndigheten i hemmedlemsstaten om en incident som inte är allvarlig blir allvarlig. I denna särskilda situation ska betaltjänstleverantörer skicka den inledande rapporten till den behöriga myndigheten direkt när denna ändrade status upptäcks, eller, vid vetskap om att den behöriga myndighetens rapporteringskanaler inte är tillgängliga eller i funktion vid denna tidpunkt, så snart som de är tillgängliga/i funktion igen.

2.10. Betaltjänstleverantörer ska bifoga övergripande information (dvs. avsnitt A i mallen) i sina inledande rapporter, dvs. grundläggande uppgifter om incidenten och dess uppskattade effekter på grundval av den information som var tillgänglig direkt efter att den upptäcktes eller omklassificerades. Om några faktiska uppgifter inte är tillgängliga ska betaltjänstleverantören företa uppskattningar. Betaltjänstleverantörer ska även ange datum för nästa uppdatering i sina inledande rapporter, vilket ska vara så snart som möjligt och under inga omständigheter senare än inom tre bankdagar.

Mellanliggande rapport

2.11. Betaltjänstleverantörer ska ge in mellanliggande rapporter varje gång de anser att det föreligger en relevant statusuppdatering och, som ett minimum, vid det datum som angetts i den föregående rapporten (antingen den inledande rapporten eller den föregående mellanliggande rapporten).

2.12. Betaltjänstleverantörer ska ge in en första mellanliggande rapport med en mer detaljerad beskrivning av incidenten och dess konsekvenser (avsnitt B i mallen) till den behöriga myndigheten. Dessutom ska betaltjänstleverantörer upprätta ytterligare mellanliggande rapporter genom att uppdatera den information som redan tillhandahållits i avsnitten A och B i mallen åtminstone när de får kännedom om ny, relevant information eller betydande förändringar sedan den föregående rapporten (t.ex. huruvida incidenten har trappats upp eller minskat i betydelse, nya orsaker har identifierats eller åtgärder har vidtagits för att lösa problemet). Betaltjänstleverantörer ska i vart fall upprätta en mellanliggande rapport på begäran från den behöriga myndigheten i hemmedlemsstaten.

2.13. Precis som för inledande rapporter ska betaltjänstleverantörer göra uppskattningar om inga faktiska uppgifter är tillgängliga.

2.14. Vidare ska betaltjänstoperatörer i varje rapport ange datum för nästa uppdatering, vilket ska vara så snart som möjligt och under inga omständigheter senare än inom tre arbetsdagar. Om det inte skulle vara möjligt för betaltjänstleverantören att iaktta det uppskattade datumet för nästa uppdatering ska betaltjänstleverantören kontakta den behöriga myndigheten för att förklara orsakerna till förseningen, föreslå en ny sannolik tidsfrist för ingivande (inte senare än inom tre arbetsdagar) och skicka en ny mellanliggande rapport som endast innehåller information om det beräknade datumet för nästa uppdatering.

2.15. Betaltjänstleverantörer ska skicka den sista mellanliggande rapporten när den reguljära verksamheten har återupptagits och driften är normal igen för att informera den behöriga myndigheten om denna omständighet. Betaltjänstleverantörer ska anse att driften är normal igen när verksamheten/driften har återgått till samma servicenivå/villkor som definierats av betaltjänstleverantören eller fastställts extern genom ett avtal om servicenivå vad gäller behandlingstider, kapacitet, säkerhetskrav osv. och det inte längre föreligger några beredskapsåtgärder.

2.16. Om driften är normal igen innan det har gått fyra timmar sedan incidenten upptäcktes ska betaltjänstleverantören sträva efter att inge både den inledande rapporten och den sista mellanliggande rapporten samtidigt (dvs. fylla i avsnitten A och B i mallen) innan tidsfristen på fyra timmar har löpt ut.

Slutrapport

2.17. Betaltjänstleverantörer ska skicka en slutrapport när analysen av de grundläggande orsakerna har ägt rum (oberoende av huruvida begränsningsåtgärder redan har genomförts

eller den slutgiltiga grundläggande orsaken har identifierats) och faktiska uppgifter är tillgängliga som kan ersätta eventuella uppskattningar.

2.18. Betaltjänstleverantörer ska ge in slutrapporten till den behöriga myndigheten senast två veckor efter det att driften anses vara normal igen. Betaltjänstleverantörer som behöver en förlängd tidsfrist (t.ex. om det inte finns några tillgängliga uppgifter om effekterna än) ska kontakta den behöriga myndigheten innan tidsfristen har löpt ut och lämna en godtagbar motivering för förseningen samt ett nytt beräknat datum för slutrapporten.

2.19. Om det är möjligt för betaltjänstleverantörer att tillhandahålla all information som krävs i slutrapporten (dvs. avsnitt C i mallen) inom fyra timmar från det att incidenten upptäcktes ska de sträva efter att i sin inledande rapport inge den information som hör samman med inledande, sista mellanliggande och slutgiltiga rapporter.

2.20. Betaltjänstleverantörer ska försöka inkludera fullständig information i sina slutrapporter, dvs. i) faktiska uppgifter om effekterna istället för uppskattningar (samt andra uppdateringar som krävs enligt avsnitten A och B i mallen) och ii) avsnitt C i mallen, vilket omfattar den grundläggande orsaken, om denna redan är känd, och en sammanfattning av vidtagna eller planerade åtgärder för att avhjälpa problemet och motverka att det återkommer i framtiden.

2.21. Betaltjänstleverantörer ska även skicka en slutrapport när de som ett resultat av den fortlöpande bedömningen av incidenten upptäcker att en redan rapporterad incident inte längre uppfyller kraven för att anses allvarlig och inte antas uppfylla dem innan incidenten avhjälps. I detta fall ska betaltjänstleverantörer skicka slutrapporten så snart som detta upptäcks och, i vilket fall som helst senast vid det uppskattade datumet för nästa rapport. I denna särskilda situation ska betaltjänstleverantören, istället för att fylla i avsnitt C i mallen, kryssa för rutan ”incident omklassificerad som mindre” och förklara skälen för denna nedgradering.

Riktlinje 3: Delegerad och konsoliderad rapportering

3.1. Om den behöriga myndigheten så medger ska betaltjänstleverantörer som önskar delegera rapporteringsskyldigheter enligt andra betaltjänstdirektivet till en tredje part informera den behöriga myndigheten i hemmedlemsstaten och säkerställa att följande villkor är uppfyllda:

a. Det formella avtalet eller, i förekommande fall, befintliga interna överenskommelser inom en koncern, som ligger till grund för den delegerade rapporteringen mellan betaltjänstleverantören och tredje part fastställer otvetydigt ansvarsfördelningen mellan samtliga parter. I synnerhet ska det tydligt anges att den berörda betaltjänstleverantören, oberoende av den eventuella delegeringen av rapporteringsskyldigheter, fortsatt kan ställas till svars fullt ut och är ansvarig för att de villkor som fastställs i artikel 96 i andra betaltjänstdirektivet är uppfyllda och för innehållet i den information som har tillhandahållits till den behöriga myndigheten i hemmedlemsstaten.

b. Delegeringen uppfyller villkoren för en utkontraktering av viktiga operativa funktioner såsom föreskrivs i

   i. artikel 19.6 i andra betaltjänstdirektivet i förhållande till betalningsinstitut och institut för elektroniska pengar, vilket ska gälla i tillämpliga delar i enlighet med artikel 3 i direktiv 2009/110/EG (e-penningdirektivet), eller

   ii. CEBS riktlinjer om utkontraktering med avseende på kreditinstitut.

c. Informationen ska ges in till den behöriga myndigheten i hemmedlemsstaten på förhand och, i vart fall, med iakttagande av tidsfrister och förfaranden som den behöriga myndigheten i förekommande fall har fastställt.

d. Sekretessen för känsliga uppgifter samt kvaliteten, samstämmigheten, integriteten och tillförlitligheten för den information som ska tillhandahållas den behöriga myndigheten säkerställs på vederbörligt sätt.

3.2. Betaltjänstleverantörer som vill utse tredje parter till att fullgöra sina rapporteringsskyldigheter på ett konsoliderat sätt (t.ex. genom att inge en enda rapport som hänför sig till flera betaltjänstleverantörer som berörs av samma allvarliga operativa eller säkerhetsincident) ska informera den behöriga myndigheten i hemmedlemsstaten, inkludera den kontaktinformation som inkluderas under ”berörd betaltjänstleverantör” i mallen och säkerställa att följande villkor är uppfyllda:

a. Denna bestämmelse ska tas in i det avtal på vilket den delegerade rapporteringen grundas.

b. Den konsoliderade rapporteringen om incidenten ska ha som villkor att den orsakats av en störning av de tjänster som tillhandahålls av tredje part.

c. Den konsoliderade rapporteringen ska begränsas till betaltjänstleverantörer som är etablerade i samma medlemsstat.

d. Det ska säkerställas att den tredje parten bedömer huruvida incidenten är allvarlig för varje berörd betaltjänstleverantör och endast inkluderar de betaltjänstleverantörer i rapporten för vilka incidenten anses vara allvarlig. Det ska vidare säkerställas att en betaltjänstleverantör, i osäkra fall, inkluderas i den konsoliderade rapporten så länge det inte föreligger några bevis för att så inte ska ske.

e. Det ska vad gäller de fält i mallen där ett gemensamt svar inte är möjligt (t.ex. avsnitt B 2, B 4 eller C 3), säkerställas att den tredje parten antingen i) fyller i dem individuellt för varje berörd betaltjänstleverantör och ytterligare specificerar identiteten från varje betaltjänstleverantör som informationen avser, eller ii) använder intervaller i de fält där detta är möjligt, med angivande av de lägsta och

högsta värden som observerats eller uppskattats för de olika betaltjänstleverantörerna.

f. Betaltjänstleverantörer ska säkerställa att tredje part ständigt håller dem informerade om all relevant information som rör incidenten och all kontakt som tredje part har haft med den behöriga myndigheten samt innehållet i denna, men endast så länge det inte innebär att skyldigheten till konfidentiell behandling åsidosätts vad gäller information som hänför sig till andra betaltjänstleverantörer.

3.3. Betaltjänstleverantörer ska inte delegera sin rapporteringsskyldighet innan de informerar den behöriga myndigheten i hemmedlemsstaten eller efter att ha informerats om att avtalet om utkontraktering inte uppfyller de krav till vilka hänvisas i riktlinje 3.1 b.

3.4. Betaltjänstoperatörer som vill återkalla delegeringen av sin rapporteringsskyldighet ska meddela detta beslut till den behöriga myndigheten i hemmedlemsstaten i enlighet med de tidsfrister och förfaranden som sistnämnda myndighet har fastställt. Betaltjänstleverantörer ska även informera den behöriga myndigheten i hemmedlemsstaten om det föreligger någon materiell utveckling som påverkar den utsedda tredje parten och dess förmåga att fullgöra rapporteringsskyldigheten.

3.5. Betaltjänstleverantörer ska väsentligen fullgöra sin rapporteringsskyldighet utan att använda extern hjälp när den utsedda tredje parten underlåter att informera den behöriga myndigheten i hemmedlemsstaten om en allvarlig operativ eller säkerhetsincident i enlighet med artikel 96 i andra betaltjänstdirektivet och dessa riktlinjer. Vidare ska betaltjänstleverantörer säkerställa att incidenter inte rapporteras två gånger, nämligen individuellt av nämnda betaltjänstleverantör och en gång till av tredje part.

Riktlinje 4: Operativ och säkerhetsrelaterad policy

4.1. Betaltjänstleverantörer ska säkerställa att allt ansvar för incidentrapportering enligt andra betaltjänstdirektivet samt de förfaranden som har antagits för att uppfylla de krav som har definierats under förevarande riktlinjer är klart definierat i deras allmänna operativa och säkerhetsrelaterade policy.

5. Riktlinjer som riktar sig till behöriga myndigheter om hur de ska bedöma incidentens relevans och vilka uppgifter i incidentrapporten som ska delas med andra inhemska myndigheter

Riktlinje 5: Bedömning av incidentens relevans

5.1. Behöriga myndigheter i hemmedlemsstaten ska bedöma den allvarliga operativa eller säkerhetsincidentens relevans för andra inhemska myndigheter, på grundval av sitt eget expertutlåtande och använda följande kriterier som huvudsakliga indikatorer för incidentens allvar:

a. Orsakerna till incidenten omfattas av den andra inhemska myndighetens regleringsbefogenheter (dvs. dess behörighetsområde).
b. Incidenten påverkar mål från en annan inhemsk myndighet (t.ex. säkerställandet av den finansiella stabiliteten).
c. Incidenten påverkar eller kan påverka betaltjänstanvändare i stor utsträckning.
d. Incidenten kommer sannolikt att få eller har fått stor uppmärksamhet i media.

5.2. Behöriga myndigheter i hemmedlemsstaten ska utföra denna bedömning kontinuerligt under den tid incidenten pågår för att upptäcka möjliga ändringar som kan innebära att en incident blir relevant som tidigare inte ansågs vara det.

Riktlinje 6: Information som ska delas

6.1. Oberoende av andra lagstadgade krav på att dela information som har samband med incidenten med andra inhemska myndigheter, ska behöriga myndigheter tillhandahålla information om allvarliga operativa eller säkerhetsincidenter till de inhemska myndigheter som identifierats med tillämpning av riktlinje 5.1 (dvs. ”andra relevanta inhemska myndigheter”), minst vid den tidpunkt när de erhåller den inledande rapporten (eller, alternativt, den rapport som föranledde delandet av information) och när de erhåller underrättelse om att verksamheten fungerar normalt igen (dvs. den sista mellanliggande rapporten).

6.2. Behöriga myndigheter ska lämna den information som behövs för att tillhandahålla en klar bild av vad som har hänt och de potentiella konsekvenserna till andra relevanta inhemska myndigheter. För att göra detta ska de åtminstone tillhandahålla den information som lämnats av betaltjänstleverantören i följande fält på mallen (antingen i den inledande eller i den mellanliggande rapporten):

- datum och tidpunkt när incidenten upptäcktes,
- datum och tidpunkt när incidenten började,
- datum och tidpunkt när incidenten återställdes eller förväntas vara återställd,
- en kortfattad beskrivning av incidenten (inbegripet de delar av den detaljerade beskrivningen som inte är känsliga),
- en kortfattad beskrivning av de åtgärder som vidtagits eller planeras att vidtas för att återhämta sig från incidenten,
- en beskrivning av hur incidenten kan påverka andra betaltjänstleverantörer och/eller infrastrukturer,
- en beskrivning (i förekommande fall) av rapporteringen i media,
- orsaken till incidenten.

6.3. Behöriga myndigheter ska, om det behövs, vidta en vederbörlig avidentifiering, och utelämna information som kan vara föremål för restriktioner på grund av konfidentialitet eller immateriella rättigheter innan den delar incidentrelaterad information med andra relevanta inhemska myndigheter. I vart fall ska behöriga myndigheter tillhandahålla den rapporterande betaltjänstleverantörens namn och adress till andra relevanta inhemska myndigheter om nämnda inhemska myndigheter kan garantera att informationen kommer att behandlas konfidentiellt.

6.4. Behöriga myndigheter ska alltid säkerställa konfidentialiteten och integriteten vad gäller den information som lagras och utväxlats med andra relevanta inhemska myndigheter och även autentisera sig själva på ett korrekt sätt i förhållande till andra relevanta inhemska myndigheter. I synnerhet ska behöriga myndigheter behandla all information som erhållits enligt dessa riktlinjer i enlighet med de krav på tystnadsplikt som föreskrivs i andra betaltjänstdirektivet, utan att det påverkar tillämplig unionsrätt och nationella krav.

6. Riktlinjer som riktar sig till behöriga myndigheter om kriterier för bedömningen av de relevanta uppgifter i incidentrapporter som ska delas med EBA och ECB samt avseende formatet och förfarandet för deras kommunikation

Riktlinje 7: Information som ska delas

7.1. Behöriga myndigheter ska alltid tillhandahålla EBA och ECB alla rapporter som erhållits från betaltjänstleverantörer (eller för deras räkning) som påverkats av en allvarlig operativ eller säkerhetsincident (dvs. inledande, mellanliggande eller slutgiltiga rapporter).

Riktlinje 8: Kommunikation

8.1. Behöriga myndigheter ska alltid säkerställa konfidentialiteten och integriteten vad gäller den information som lagrats och utväxlats med EBA och ECB och även autentisera sig själva på ett korrekt sätt i förhållande till EBA och ECB. I synnerhet ska behöriga myndigheter behandla all information som erhållits enligt dessa riktlinjer i enlighet med de krav på tystnadsplikt som föreskrivs i andra betaltjänstdirektivet, utan att det påverkar tillämplig unionsrätt och nationella krav.

8.2. För att undvika förseningar vid överföringen av incidentrelaterad information till EBA/ECB och bidra till att minimera risker för driftsavbrott bör behöriga myndigheter stödja lämpliga kommunikationsmedel.

Bilaga 1 – Rapporteringsmallar för betaltjänstleverantörer

CLASSIFICATION: RESTRICTED

Major Incident Report

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

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

A - Initial report

A 1 - GENERAL DETAILS					
Type of report					
Type of report	☐ Individual	☐ Consolidated			
Affected payment service provider (PSP)					
PSP name					
PSP unique identification number, if relevant					
PSP authorisation number					
Head of group, if applicable					
Home country					
Country/countries affected by the incident					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	
Reporting entity (complete this section if the reporting entity is not the affected PSP in case of delegated reporting)					
Name of the reporting entity					
Unique identification number, if relevant					
Authorisation number, if applicable					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	

A 2 - INCIDENT DETECTION and INITIAL CLASSIFICATION			
Date and time of detection of the incident	DD/MM/YYYY, HH:MM		
The incident was detected by (1)		If Other, please explain:	
Please provide a short and general description of the incident (should you deem the incident to have an impact in other EU Member States(s), and if feasible within the applicable reporting deadlines, please provide a translation in English)			
What is the estimated time for the next update?	DD/MM/YYYY, HH:MM		

B - Intermediate report

B 1 - GENERAL DETAILS

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

B 2 - INCIDENT CLASSIFICATION & INFORMATION ON THE INCIDENT

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

B 3 - INCIDENT DESCRIPTION

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

B 4 - INCIDENT IMPACT

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

B 5 - INCIDENT MITIGATION

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

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

Notes:

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

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

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

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

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

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

INSTRUKTIONER FÖR IFYLLANDET AV MALLARNA

Betaltjänstleverantörer ska fylla i de relevanta avsnitten i mallen, beroende på vilken rapporteringsfas de befinner sig i, nämligen avsnitt A för den inledande rapporten, avsnitt B för mellanliggande rapporter och avsnitt C för slutrapporten. Alla fält är obligatoriska såvida inte något annat uttryckligen anges.

Rubrik

Inledande rapport: detta är den första anmälan som betaltjänstleverantören gör till den behöriga myndigheten i hemmedlemsstaten.

Mellanliggande rapport: detta utgör en uppdatering av en tidigare (inledande eller mellanliggande) rapport om samma incident.

Sista mellanliggande rapport: genom denna rapport underrättas den behöriga myndigheten i hemmedlemsstaten om att den normala verksamheten har återupptagits och att inga fler mellanliggande rapporter kommer att inges.

Slutrapport: det är den sista rapporten som betaltjänstleverantören kommer att skicka om incidenten, eftersom i) en analys av de grundläggande orsakerna redan har genomförts och uppskattningarna kan ersättas med riktiga siffror eller ii) incidenten inte längre anses vara allvarlig.

Incidenten har omklassificerats som mindre allvarlig: Incidenten uppfyller inte längre villkoren för att anses allvarlig och förväntas inte uppfylla dem innan den har avhjälpts. Betaltjänstleverantören ska ange skälen till denna nedgradering.

Datum och tid för rapporten: exakt datum och tid för ingivande av rapporten till den behöriga myndigheten.

Incidentens identifikationsnummer, i tillämpliga fall (för mellanliggande och slutgiltiga rapporter): det referensnummer som den behöriga myndigheten har utfärdat vid tidpunkten för den inledande rapporten för en unik identifiering av incidenten, i förekommande fall (dvs. om en sådan referens tillhandahålls av den behöriga myndigheten).

A – Inledande rapport

A 1 – Allmänna uppgifter

Typ av rapport:

Individuell: rapporten hänför sig till en enskild betaltjänstleverantör.

Konsoliderad: Rapporten hänför sig till flera betaltjänstleverantörer som utnyttjar möjligheten till konsoliderad rapportering. Fälten under ”Berörd betaltjänstleverantör” ska lämnas tomma (med undantag för fältet ”Land/länder som berörs av incidenten”) och en förteckning över de betaltjänstleverantörer som rapporten omfattar ska tillhandahållas genom att den motsvarande tabellen (Konsoliderad rapport – förteckning över betaltjänstleverantörer) fylls i.

Berörd betaltjänstleverantör: hänför sig till den betaltjänstleverantör som har drabbats av incidenten.

Leverantörens namn: fullständigt namn på den betaltjänstleverantör som är föremål för rapporteringsförfarandet såsom det anges i det tillämpliga officiella nationella registret över betaltjänstleverantörer.

Leverantörens unika registreringsnummer, i förekommande fall: det relevanta, unika identifikationsnummer som används i varje medlemsstat för att identifiera betaltjänstleverantören, vilket betaltjänstleverantören ska tillhandahålla om fältet ”Leverantörens auktorisationsnummer” inte har fyllts i.

Leverantörens auktorisationsnummer: hemmedlemsstatens auktorisationsnummer.

Koncernchef: I fråga om koncerner, såsom de definieras i artikel 4.40 i Europaparlamentets och rådets direktiv 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden och om ändring av direktiven 2002/65/EG, 2009/110/EG, 2013/36/EG samt förordning (EU) nr 1093/2010 samt upphävande av direktiv 2007/64/EG, var god ange koncernchefens namn.

Hemmedlemsstat: medlemsstat där betaltjänstleverantörens säte är beläget, eller om betaltjänstleverantören enligt nationell rätt saknar säte, den medlemsstat där dess huvudkontor är beläget.

Land/länder som berörs av incidenten: Land eller länder som har berörts av incidenten (t.ex. flera filialer från en betaltjänstleverantör som är belägna i olika länder berörs). Kan, men behöver inte vara samma som hemmedlemsstaten.

Primär kontaktperson: förnamn och efternamn på den person som är ansvarig för att rapportera incidenten eller, om en tredje part rapporterar för den berörda betaltjänstleverantörens räkning, förnamn och efternamn på den person som är ansvarig för avdelningen för incidenthantering/risk eller liknande område vid den berörda betaltjänstleverantören.

E-post: E-postadress till vilken förfrågningar om ytterligare klargörande kan riktas, i förekommande fall. Det kan antingen vara en personlig e-postadress eller en företagsadress.

Telefon: Telefonnummer att ringa vid förfrågningar om ytterligare klargörande, i förekommande fall. Det kan antingen vara ett personligt nummer eller ett företagsnummer.

Sekundär kontaktperson: Förnamn och efternamn på en alternativ person som den behöriga myndigheten kan kontakta vid förfrågningar om incidenten om den primära kontaktpersonen inte är tillgänglig. Om en tredje part rapporterar för den berörda betaltjänstleverantörens räkning, förnamn och efternamn på en alternativ person vid avdelningen för incidenthantering/risk eller liknande område vid den berörda betaltjänstleverantören.

E-post: E-postadress till den alternativa kontaktperson till vilken förfrågningar om ytterligare klargörande kan riktas, i förekommande fall. Det kan antingen vara en personlig e-postadress eller en företagsadress.

Telefon: Telefonnummer till den alternativa kontaktpersonen att ringa vid förfrågningar om ytterligare klargörande, i förekommande fall. Det kan antingen vara ett personligt nummer eller ett företagsnummer.

Rapporterande enhet: denna avdelning ska fyllas i om en tredje part uppfyller rapporteringsskyldigheten för den berörda betaltjänstleverantörens räkning.

Den rapporterande enhetens namn: fullständigt namn på den enhet som rapporterar incidenten såsom det anges i det tillämpliga officiella nationella företagsregistret.

Unikt identifikationsnummer, i förekommande fall: det relevanta, unika identifikationsnummer som används i det land där tredje part är etablerad för att identifiera den enhet som rapporterar incidenten. Ska tillhandahållas av den rapporterande enheten om fältet ”Auktorisationsnummer” inte har fyllts i.

Auktorisationsnummer, i förekommande fall: auktorisationsnumret från den tredje parten i det land där den tredje parten är etablerad, i förekommande fall.

Primär kontaktperson: förnamn och efternamn på den person som är ansvarig för att rapportera incidenten.

E-post: E-postadress till vilken förfrågningar om ytterligare klargörande kan riktas, i förekommande fall. Det kan antingen vara en personlig e-postadress eller en företagsadress.

Telefon: Telefonnummer att ringa vid förfrågningar om ytterligare klargörande, i förekommande fall. Det kan antingen vara ett personligt nummer eller ett företagsnummer.

Sekundär kontaktperson: förnamn och efternamn på en alternativ person från enheten som rapporterar incidenten som den behöriga myndigheten kan kontakta när den primära kontaktpersonen inte är tillgänglig.

E-post: E-postadress till den alternativa kontaktperson till vilken förfrågningar om ytterligare klargörande kan riktas, i förekommande fall. Det kan antingen vara en personlig e-postadress eller en företagsadress.

Telefon: Telefonnummer till den alternativa kontaktpersonen att ringa vid förfrågningar om ytterligare klargörande, i förekommande fall. Det kan antingen vara ett personligt nummer eller ett företagsnummer.

A 2 – Upptäckt av incidenten och inledande klassificering

Datum och tid när incidenten upptäcktes: datum och tid när incidenten identifierades första gången.

Incidenten upptäcktes av: Ange huruvida incidenten upptäcktes av en betaltjänstanvändare, av någon annan part som tillhör betaltjänstleverantören (t.ex. intern revision) eller en extern part (t.ex. en extern tjänsteleverantör). Om det inte var någon av dessa, var god tillhandahåll en förklaring i motsvarande fält.

Kortfattad och allmän beskrivning av incidenten: redogör kortfattat för de mest relevanta omständigheterna, inbegripet möjliga orsaker, omedelbara effekter, etc.

Beräknad tidpunkt för nästa uppdatering: ange beräknat datum och tidpunkt för ingivandet av nästa uppdatering (mellanliggande eller slutgiltig rapport).

B – Mellanliggande rapport

B 1 – Allmänna uppgifter

Mer detaljerad beskrivning av incidenten: beskriv incidentens huvuddrag, åtminstone de punkter som anges i frågeformuläret (vilket specifikt problem betaltjänstleverantören står inför, hur det började och utvecklades, möjlig koppling till en tidigare incident, konsekvenser, särskilt för betaltjänstanvändare, osv.).

Datum och tidpunkt när incidenten började: datum och tidpunkt när incidenten började, om detta är känt.

Incidentstatus:

Diagnostik: incidentens grundläggande egenskaper har just identifierats.

Avhjälpande: de attackerade delarna håller på att omkonfigureras.

Återvinning: de felaktiga delarna återställs till sitt sista återställbara tillstånd.

Återställning: den betalningsrelaterade tjänsten tillhandahålls igen.

Datum och tidpunkt när incidenten återställdes eller förväntas vara återställd: ange datum och tidpunkt när incidenten var eller förväntas vara under kontroll och verksamheten var eller förväntas vara normal igen.

B 2 – Klassificering av incidenten/information om incidenten

Sammanlagd effekt: Var god ange vilka kriterier som har påverkats av incidenten. Flera rutor får kryssas för.

Integritet: innebär ett säkerställande att tillgångarna (inbegripet data) är korrekta och fullständiga.

Tillgänglighet: innebär att betalningsrelaterade tjänster är tillgängliga och kan användas av betaltjänstanvändarna.
Konfidentialitet: innebär att information inte görs tillgänglig eller lämnas ut till icke auktoriserade personer, enheter eller förfaranden.
Autenticitet: innebär att en källa är vad den utger sig för att vara.
Kontinuitet: innebär att de processer, uppgifter och tillgångar som en organisation behöver för att leverera betalningsrelaterade tjänster är fullt tillgängliga och fungerar på i förväg fastställda godtagbara nivåer.

Berörda transaktioner: Betaltjänstleverantörer ska ange vilka trösklar som uppnås eller sannolikt kommer att uppnås genom incidenten, i förekommande fall, och relaterade siffror: antalet berörda transaktioner, procentandelen berörda transaktioner i förhållande till antalet betalningstransaktioner som utförs med samma betaltjänst som har påverkats av incidenten och transaktionernas totala värde. Betaltjänstleverantörer ska tillhandahålla särskilda värden för dessa variabler, vilka antingen kan utgöra faktiska siffror eller uppskattningar. Enheter som rapporterar för flera betaltjänstleverantörers räkning (dvs. konsoliderad rapportering) kan istället tillhandahålla värdeintervaller som representerar de lägsta och högsta värden som observerats eller uppskattats inom den grupp av betaltjänstleverantörer som rapporten avser, separerade med ett bindestreck. I allmänhet bör betaltjänstleverantörer tolka ”berörda transaktioner” som alla inhemska och gränsöverskridande transaktioner som direkt eller indirekt har påverkats eller sannolikt kommer att påverkas av incidenten och, i synnerhet, transaktioner som inte kunde initieras eller behandlas, sådana där innehållet i betalningsmeddelandet ändrats och sådana som beställts i bedrägligt syfte (oberoende av huruvida medlen har återvunnits eller inte). Vidare ska betaltjänstleverantörer tolka den normala nivån av betalningstransaktioner som det dagliga årliga genomsnittet av inhemska och gränsöverskridande betalningstransaktioner som genomförs med samma betaltjänst som har påverkats av incidenten, med föregående år som referensperiod för beräkningarna. Om betaltjänstleverantörer inte anser att denna siffra är representativ (t.ex. på grund av säsongsvariationer), ska de använda en annan, mer representativ parameter och informera den behöriga myndigheten om de underliggande skälen för detta tillvägagångssätt i fältet ”Kommentarer”.

Berörda betaltjänstanvändare: Betaltjänstleverantörer ska ange vilka trösklar som uppnås eller sannolikt kommer att uppnås genom incidenten, i förekommande fall, och relaterade siffror: totalt antal berörda betaltjänstanvändare och procentandelen berörda betaltjänstanvändare i förhållande till det totala antalet betaltjänstanvändare. Betaltjänstleverantörer ska tillhandahålla konkreta värden för dessa variabler, vilka antingen kan utgöra faktiska siffror eller uppskattningar. Enheter som rapporterar för flera betaltjänstleverantörers räkning (dvs. konsoliderad rapportering) kan istället tillhandahålla värdeintervaller som representerar de lägsta och högsta värden som observerats eller uppskattats inom den grupp av betaltjänstleverantörer som rapporten avser, separerade med ett bindestreck. Betaltjänstleverantörer ska tolka ”berörda betaltjänstanvändare” som samtliga kunder (antingen inhemska eller utländska, konsumenter eller företag) som har ett avtal med den berörda betaltjänstleverantören som ger dem tillgång till den berörda betaltjänsten, och som har drabbats eller sannolikt kommer att drabbas av konsekvenserna av incidenten. Betaltjänstleverantörer ska göra uppskattningar som grundas på deras tidigare verksamhet för att fastställa det antal betaltjänstanvändare som kan ha använt betaltjänsten under den tid som incidenten pågick. Vad gäller koncerner ska varje betaltjänstleverantör endast beakta sina egna betaltjänstanvändare. Om en betaltjänstleverantör erbjuder operativa tjänster till andra ska den betaltjänstleverantören endast beakta sina egna betaltjänstanvändare (om det föreligger sådana) och betaltjänstleverantörer som tar emot dessa operativa tjänster ska bedöma incidenten i förhållande till sina egna betaltjänstanvändare. Vidare ska betaltjänstleverantörer tolka det totala antalet betaltjänstanvändare som det sammanlagda

antalet inhemska och gränsöverskridande betaltjänstanvändare som var bundna genom avtal till dem när incidenten inträffade (eller, alternativt, de senaste tillgängliga sifferuppgifterna) och hade tillgång till den berörda betaltjänsten, oberoende av deras storlek eller huruvida de anses utgöra aktiva eller passiva betaltjänstanvändare.

Driftavbrott: Betaltjänstleverantörer ska ange om tröskeln har uppnåtts eller sannolikt kommer att uppnås genom incidenten och den relaterade siffran: totalt driftavbrott. Betaltjänstleverantörer ska tillhandahålla konkreta värden för denna variabel, vilka antingen kan utgöra faktiska siffror eller uppskattningar. Enheter som rapporterar för flera betaltjänstleverantörers räkning (dvs. konsoliderad rapportering) kan istället tillhandahålla värdeintervaller som representerar de lägsta och högsta värden som observerats eller uppskattats inom den grupp av betaltjänstleverantörer som rapporten avser, separerade med ett bindestreck. Betaltjänstleverantörer ska beakta den period som varje uppgift, process eller kanal med anknytning till tillhandahållandet av betaltjänster är eller sannolikt kommer att vara ur funktion och således utgör hinder mot i) initiering och/eller genomförande av en betaltjänst och/eller ii) tillgång till ett betalkonto. Betaltjänstleverantörer ska räkna driftavbrottet från den tidpunkt det uppkommer och beakta såväl tidsintervaller när de är öppna för handel såsom krävs för genomförandet av betaltjänster som intervaller när de är stängda och underhållsperioder, om det är relevant och i förekommande fall. Om betaltjänstleverantörer inte kan fastställa när driftavbrottet inträffade ska de undantagsvis beräkna det från den tidpunkt när det upptäcktes.

Ekonomiska effekter: Betaltjänstleverantörer ska ange om tröskeln har uppnåtts eller sannolikt kommer att uppnås genom incidenten och de relaterade siffrorna: direkta kostnader och indirekta kostnader. Betaltjänstleverantörer ska tillhandahålla konkreta värden för dessa variabler, vilka antingen kan utgöra faktiska siffror eller uppskattningar. Enheter som rapporterar för flera betaltjänstleverantörers räkning (dvs. konsoliderad rapportering) kan istället tillhandahålla värdeintervaller som representerar de lägsta och högsta värden som observerats eller uppskattats inom den grupp av betaltjänstleverantörer som rapporten avser, separerade med ett bindestreck. Betaltjänstleverantörer ska beakta både kostnader som har en direkt anknytning till incidenten och sådana som har en indirekt anknytning till incidenten. Betaltjänstleverantörer ska bland annat beakta exproprierade medel eller tillgångar, kostnader för utbyte av maskin- eller programvara, andra juridiska kostnader eller kostnader för avhjälpande, avgifter på grund av åsidosättande av avtalsförpliktelser, sanktioner, externa skulder och förlorade intäkter. Vad gäller indirekta kostnader ska betaltjänstleverantörerna endast beakta kostnader som redan är kända eller med stor sannolikhet kommer att dyka upp.

> **Direkta kostnader:** penningbelopp (euro) som direkt orsakas av incidenten, inbegripet medel som krävs för att avhjälpa incidenten (t.ex. exproprierade medel eller tillgångar, kostnader för utbyte av maskin- eller programvara, avgifter på grund av åsidosättande av avtalsförpliktelser).
>
> **Indirekta kostnader:** penningbelopp (euro) som indirekt orsakats av incidenten (t.ex. kostnader för ersättning/kompensation till kunder, förlorade intäkter till följd av förlorade affärsmöjligheter, eventuella rättsliga kostnader).

Hög intern upptrappningsnivå: Betaltjänstleverantörer ska beakta huruvida den informationsansvariga (eller en person i liknande ställning) har informerats eller sannolikt kommer att informeras om incidenten på grund av dess påverkan på betalningsrelaterade tjänster utöver vid ett eventuellt periodiskt anmälningsförfarande samt kontinuerligt under den tid incidenten pågick. Vad gäller delegerad rapportering skulle upptrappningen äga rum hos tredje part. Dessutom ska betaltjänstleverantörer beakta huruvida ett krisläge har utlösts eller sannolikt kommer att utlösas som ett resultat av incidentens påverkan på betalningsrelaterade tjänster.

Andra betaltjänstleverantörer eller relevanta infrastrukturer som kan beröras: Betaltjänstleverantörer ska bedöma incidentens påverkan på den finansiella marknaden, vilken ska tolkas som den finansiella marknadens infrastrukturer och/eller kortbetalningssystem som stödjer den och andra betaltjänstleverantörer. I synnerhet ska betaltjänstleverantörer bedöma huruvida incidenten har spridit sig eller sannolikt kommer att sprida sig till andra betaltjänstleverantörer, huruvida den har påverkat eller sannolikt kommer att påverka att infrastrukturerna på den finansiella marknaden fungerar väl och huruvida den har äventyrat eller sannolikt kommer att äventyra hela det finansiella systemets soliditet. Betaltjänstleverantörer ska ta hänsyn till olika parametrar såsom huruvida den berörda komponenten/programvaran är privatägd eller tillgänglig för allmänheten, huruvida det äventyrade nätverket är internt eller externt och huruvida betaltjänstleverantören har slutat fullgöra eller sannolikt kommer att sluta fullgöra sina skyldigheter i de finansiella marknadsinfrastrukturer där betaltjänstleverantören är medlem.

Effekter på anseendet: Betaltjänstleverantörer ska beakta hur synlig incidenten, såvitt de vet, har blivit eller sannolikt kommer att bli på marknaden. I synnerhet ska betaltjänstleverantörer beakta hur sannolikt det är att incidenten kommer att skada samhället som en bra indikator på dess potentiella effekter på deras anseende. Betaltjänstleverantörer ska beakta huruvida i) incidenten har påverkat en synlig process och därför sannolikt kommer att uppmärksammas eller redan har uppmärksammats i media (inte endast med beaktande av traditionella media, såsom tidningar, utan även bloggar, sociala nätverk etc.), ii) skyldigheter enligt lag har åsidosatts eller sannolikt kommer att åsidosättas, iii) sanktioner som har åsidosatts eller sannolikt kommer att åsidosättas eller iv) samma typ av incident har inträffat tidigare.

B 3 – Beskrivning av incidenten

Typ av incident: ange huruvida det, såvitt ni kan bedöma, är frågan om en operativ incident eller en säkerhetsincident.

Operativ: incidenten härrör från olämpliga eller bristfälliga processer, personer och system eller force majeure som påverkar de betalningsrelaterade tjänsternas integritet, tillgänglighet, konfidentialitet, autenticitet och/eller kontinuitet.

Säkerhet: Icke auktoriserad tillgång, användning, offentliggörande, störning, ändring eller förstörelse av betaltjänstleverantörens tillgångar som påverkar de betalningsrelaterade tjänsternas integritet, tillgänglighet, konfidentialitet, autenticitet och/eller kontinuitet. Detta kan bland annat inträffa vid cyberattacker mot betaltjänstleverantören, bristfällig design eller bristfälligt genomförande av säkerhetspolicyer, eller otillräcklig fysisk säkerhet.

Orsaken till incidenten: Ange orsaken till incidenten eller, om den ännu inte är känd, den mest sannolika orsaken. Flera rutor får kryssas för.

Under utredning: orsaken har inte fastställts än.

Extern attack: orsaken kommer från en extern källa och riktar sig uppsåtligen mot betaltjänstleverantören (t.ex. angrepp genom sabotageprogram).

Intern attack: orsaken kommer från en intern källa och riktar sig uppsåtligen mot betaltjänstleverantören (t.ex. internt bedrägeri).

Typ av attack:

Överbelastningsattack (D/DoS): ett försök att göra en onlinetjänst otillgänglig genom att överbelasta den med trafik från flera olika källor.

Infektion av interna system: skadliga åtgärder som attackerar datasystem och försöker att stjäla plats på hårddisken eller processortid, få tillgång till privat information, skada data, skicka skräppost till kontakter etc.

Riktat intrång: icke auktoriserat spionage, snokande och stöld av information via cyberrymden.

Annat: Någon annan typ av attack som betaltjänstleverantören har utsatts för, antingen direkt eller genom en tjänsteleverantör. Denna ruta ska i synnerhet kryssas för om det har förekommit en attack som riktar sig mot tillståndsförfarandet eller autentiseringsförfarandet. Uppgifter ska bifogas i fritextfältet.

Externa händelser: orsaken är kopplad till händelser som generellt sett är utanför organisationens kontroll (t.ex. naturkatastrofer, rättsliga frågor, affärsfrågor och beroendet av tjänster).

Mänskligt fel: incidenten orsakades av ett oavsiktligt misstag från en person, antingen som del av betalningsförfarandet (t.ex. uppladdning av fel kommandofil för betalningar i betalningssystemet) eller på något sätt kopplat till det (t.ex. strömmen bryts av misstag och betalningsverksamheten får vänta).

Processfel: orsaken till incidenten var bristfällig design eller ett bristfälligt genomförande av betalningsprocessen, processregleringssystemet och/eller stödjande processer (t.ex. för ändring/migrering, testning, konfigurering, kapacitet, övervakning).

Systemfel: orsaken till incidenten är kopplad till bristfällighet i frågan om design, genomförande, komponenter, specifikationer, integration eller komplexitet hos de system som stödjer betalningsverksamheten.

Annat: Orsaken till incidenten är inte något av ovanstående. Ytterligare uppgifter ska tillhandahållas i fritextfältet.

Påverkade incidenten er direkt eller indirekt genom en tjänsteleverantör?: En incident kan vara direkt riktad till en betaltjänstleverantör eller påverka betaltjänstleverantören indirekt genom en tredje part. Om det är frågan om indirekt påverkan, var god ange namnet på tjänsteleverantören/leverantörerna.

B 4 – Incidentens effekter

Berörd(a) byggnad(er) (adress), i förekommande fall: om en fysisk byggnad berörs, var god ange dess adress.

Berörda kommersiella kanaler: Ange den kanal/de kanaler för samverkan med betaltjänstanvändare som har berörts av incidenten. Flera rutor får kryssas för.

Filialer: Driftsställe (annat än huvudkontoret) som utgör en del av ett betalningsinstitut, inte är en juridisk person och självständigt genomför alla eller vissa av de transaktioner som hänför sig till betaltjänstleverantörens verksamhet. Alla driftsställen som har inrättats i samma medlemsstat av en betaltjänstleverantör med huvudkontor i en annan medlemsstat ska betraktas som en enda filial.

Internetbanktjänster: genomförande av finansiella transaktioner på internet med användning av datorer.

Telefonbanktjänster: genomförande av finansiella transaktioner med användning av telefoner.

Mobila banktjänster: genomförande av finansiella transaktioner med användning av en särskild bankapp på en smarttelefon eller liknande apparat för att utföra finansiella transaktioner.

Uttagsautomater: elektromekaniska anordningar som gör det möjligt för betaltjänstanvändare att ta ut kontanter från sina konton och/eller få tillgång till andra tjänster.

Försäljningsställe: fysiska lokaler från näringsidkaren där betaltransaktioner initieras.

Annat: Den berörda kommersiella kanalen är inget av ovanstående. Ytterligare uppgifter ska tillhandahållas i fritextfältet.

Berörda betaltjänster: Ange vilka betaltjänster som inte fungerar korrekt till följd av incidenten. Flera rutor får kryssas för.

Kontantinsättning på ett betalkonto: inlämning av kontanter till en betaltjänstleverantör för att de ska krediteras på ett betalkonto.

Kontantuttag från ett betalkonto: en begäran som betaltjänstleverantören erhåller från dess betaltjänstanvändare att tillhandahålla kontanter och debitera hans/hennes betalkonto med motsvarande summa.

Transaktioner som krävs för att förvalta ett betalkonto: de transaktioner som behöver vidtas för att aktivera, avaktivera och/eller bibehålla ett betalkonto (t.ex. öppnande, blockering).

Förvärv av betalningsinstrument: en betaltjänst som innebär att en betaltjänstleverantör har ingått avtal med en betalningsmottagare om att acceptera och behandla betalningstransaktioner och som medför en överföring av medel till betalningsmottagaren.

Betalning: en betaltjänst för kreditering av en betalningsmottagares betalkonto med en betalningstransaktion eller en rad betalningstransaktioner från en betalares betalkonto, som utförs av en betaltjänstleverantör som har tillgång till betalarens betalkonto på grundval av en instruktion som lämnats av betalaren.

Autogiro: en betaltjänst för debitering av en betalares betalkonto, där en betalningstransaktion initieras av betalningsmottagaren på grundval av betalarens medgivande till betalningsmottagaren, betalningsmottagarens betaltjänstleverantör eller betalarens egen betaltjänstleverantör.

Kortbetalning: En betaltjänst som grundas på kontokortsystemets infrastruktur och uppföranderegler för att göra en betalningstransaktion via kort, telekommunikation, digital- eller IT-utrustning, eller programvara om detta medför en betal- eller kreditkortstransaktion. Kortbaserade betalningstransaktioner omfattar inte transaktioner som baseras på andra former av betaltjänster.

Utfärdande av betalningsinstrument: en betaltjänst som innebär att en betaltjänstleverantör har ingått avtal med en betalare om att tillhandahålla betalaren ett betalningsinstrument för att initiera och behandla betalarens betalningstransaktioner.

Penningöverföring: en betaltjänst där medel erhålls från en betalare, utan att några betalkonton upprättas i betalarens eller betalningsmottagarens namn, med enda syfte att överföra motsvarande belopp till en betalare eller till en annan betaltjänstleverantör som agerar på betalningsmottagarens vägnar, och/eller där sådana medel erhålls på betalningsmottagarens vägnar och görs tillgängliga för betalningsmottagaren.

Betalningsinitieringstjänster: betaltjänster för att initiera en betalningsorder på betaltjänstanvändarens begäran med avseende på ett betalkonto som innehas hos en annan betaltjänstleverantör.

Kontoinformationstjänster: en onlinebetaltjänst för att tillhandahålla sammanställd information om ett eller flera betalkonton som betaltjänstanvändaren antingen innehar hos en annan betaltjänstleverantör eller hos fler än en betaltjänstleverantör.

Annat: Den berörda betaltjänsten är ingen av de ovanstående. Ytterligare uppgifter ska tillhandahållas i fritextfältet.

Berörda funktionsområden: Ange det eller de steg i betalningsprocessen som incidenten har påverkat. Flera rutor får kryssas för.

Autentisering/auktorisation: Ett förfarande genom vilket en betaltjänstleverantör kan kontrollera en betaltjänstanvändares identitet eller giltighet när det gäller användningen av ett specifikt betalningsinstrument, inklusive användningen av användarens personliga säkerhetsbehörighetsuppgifter och att betaltjänstanvändaren (eller en tredje part som agerar för användarens räkning) ger sitt samtycke till att överföra medel eller värdepapper.

Kommunikation: informationsflöde som används för identifiering, autentisering, meddelanden och information mellan den kontoförvaltande betaltjänstleverantören och leverantörer av betalningsinitieringstjänster, leverantörer av kontoinformationstjänster, betalare, betalningsmottagare och andra betaltjänstleverantörer.

Clearing: ett förfarande för att överföra, avsluta och, i vissa fall, bekräfta överföringsorder innan de avvecklas, eventuellt omfattande kvittning av order och fastställande av slutlig avvecklingspositioner.

Direkt avveckling: slutförandet av en transaktion eller av en behandling i syfte att reglera deltagarnas förpliktelser genom överföring av medel om denna åtgärd genomförs av den berörda betaltjänstleverantören själv.

Indirekt avveckling: slutförandet av en transaktion eller av en behandling i syfte att reglera deltagarnas förpliktelser genom överföring av medel om denna åtgärd genomförs av en annan betaltjänstleverantör för den berörda betaltjänstleverantörens räkning.

Annat: Det berörda funktionsområdet är inget av de ovanstående. Ytterligare uppgifter ska tillhandahållas i fritextfältet.

Berörda system och komponenter: Ange vilken del eller vilka delar av betaltjänstleverantörens tekniska infrastruktur som incidenten har påverkat. Flera rutor får kryssas för.

Applikation/programvara: program, operativsystem, etc. som stödjer betaltjänstleverantörens tillhandahållande av betaltjänster.

Databas: datastruktur som lagrar personlig information och betalningsinformation som behövs för att genomföra betalningstransaktioner.

Maskinvara: fysisk teknisk utrustning som sköter processerna och/eller lagrar de uppgifter som betaltjänstleverantörerna behöver för att utföra sin betalningsrelaterade verksamhet.

Nätverk/infrastruktur: telekommunikationsnätverk, antingen offentliga eller privata som medger utbyte av uppgifter och information under betalningsprocessen (t.ex. internet).

Annat: Det berörda systemet eller komponenten är inget av ovanstående. Ytterligare uppgifter ska tillhandahållas i fritextfältet.

Berörd personal: Ange huruvida incidenten har påverkat betaltjänstleverantörens personal och tillhandahåll i så fall uppgifter i fritextfältet.

B 5 – Begränsning av incidenten

Vilka handlingar/åtgärder har vidtagits hittills eller är planerade för att återhämta sig från incidenten?: lämna uppgifter om vilka åtgärder som har vidtagits eller planeras att vidtas för att tillfälligt åtgärda incidenten.

Har kontinuitetsplaner och/eller katastrofplaner aktiverats?: ange om detta är fallet och tillhandahåll i förekommande fall de mest relevanta uppgifterna om vad som har hänt (t.ex. när de aktiverades och innehållet i dessa planer).

Har leverantören dragit in eller försvagat vissa kontroller på grund av incidenten?: ange huruvida betaltjänstleverantören har varit tvungen att slopa vissa kontroller (t.ex. slopad

användning av principen om fyra ögon) för att åtgärda incidenten och tillhandahåll i så fall uppgifter om de bakomliggande skälen för att motivera de försvagade eller indragna kontrollerna.

C – Slutrapport

C 1 – Allmänna uppgifter

Uppdatering av informationen i den mellanliggande rapporten (sammanfattning): var god tillhandhåll ytterligare information om de åtgärder som har vidtagits för att återhämta sig från incidenten och undvika att den återkommer, analys av de grundläggande orsakerna, lärdomar som dragits etc.

Datum och tidpunkt när incidenten avslutades: ange datum och tid när incidenten ansågs avslutad.

Är de ursprungliga kontrollerna på plats igen?: om betaltjänstleverantören var tvungen att dra in eller försvaga några kontroller på grund av incidenten, ange huruvida dessa kontroller tillämpas igen och tillhandahåll ytterligare information i fritextfältet.

C 2 – Analys av de grundläggande orsakerna och uppföljning

Vilken var den grundläggande orsaken, om den redan är känd?: Förklara vilken som var den grundläggande orsaken till incidenten eller, om den ännu inte är känd, de preliminära slutsatser som dragits av analysen av de grundläggande orsakerna. Betaltjänstleverantörer får bifoga en fil med detaljerad information om de anser att det behövs.

Huvudsakliga korrigerande handlingar/åtgärder som vidtagits eller planeras för att förhindra att incidenten inträffar igen i framtiden, om de redan är kända: var god beskriv de huvudsakliga åtgärder som har vidtagits eller planeras att vidtas för att förhindra att incidenten inträffar igen i framtiden.

C 3 – Ytterligare information

Har incidenten delats med andra betaltjänstleverantörer i informationssyfte?: tillhandahåll en översikt över vilka betaltjänstleverantörer som har kontaktats, antingen formellt eller informellt, för att informera dem om incidenten, med uppgifter om vilka betaltjänstleverantörer som har informerats, vilken information som har utväxlats och de underliggande skälen för utväxlingen av denna information.

Har rättsliga åtgärder vidtagits mot leverantören?: var god ange huruvida betaltjänstleverantören, vid den tidpunkt slutrapporten fylls i, har blivit föremål för rättsliga åtgärder (t.ex. har ställts inför rätta eller förlorat sin licens) till följd av incidenten.