EBA/GL/2021/03

10 juni 2021

Reviderade riktlinjer

för rapportering vid allvarliga incidenter enligt andra betaltjänstdirektivet

1. Efterlevnad och rapporteringsskyldigheter

Riktlinjernas status

1. Detta dokument innehåller riktlinjer som utfärdats enligt artikel 16 i EBA-förordningen[1]. Enligt artikel 16.3 i EBA-förordningen ska de behöriga myndigheterna och finansinstituten med alla tillgängliga medel söka följa riktlinjerna.

2. Av riktlinjerna framgår 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 EBA-förordningen 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 EBA-förordningen ska de behöriga myndigheterna meddela EBA att de följer eller tänker följa dessa riktlinjer, eller i annat fall, senast den (07.11.2021), ange skälen till att de inte gör det. Om någon sådan anmälan inte inkommer inom denna tidsfrist, kommer EBA att anse att de behöriga myndigheterna inte följer riktlinjerna. Anmälningar bör lämnas in på det formulär som tillhandahålls på EBA:s webbsida, med hänvisningen ”EBA/GL/2021/03”. 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 andra betaltjänstdirektivet 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 andra betaltjänstdirektivet.

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).

12. Dessa riktlinjer är även tillämpliga när allvarliga incidenter påverkar funktioner som utkontrakterats till tredje part av betaltjänstleverantörer.

Adressater

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

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

Definitioner

15. Om inte annat anges har de termer som används och definieras i andra betaltjänstdirektivet samma betydelse i riktlinjerna. Dessutom gäller följande definitioner i dessa riktlinjer:

Operativa incidenter 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 och/eller autenticitet.
Integritet	Innebär ett säkerställande av att tillgångarna (inbegripet data) är korrekta och fullständiga.
Tillgänglighet	Innebär att betaltjänster är fullt tillgängliga och användbara av betaltjänstanvändarna enligt de accepterade nivåer som på förhand definierats av betaltjänstensleverantören.
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.
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

16. Dessa riktlinjer gäller från den 1 januari 2022.

Upphävande

17. Följande riktlinjer upphör att gälla från den 1 januari 2022:

Riktlinjer för rapportering vid allvarliga incidenter enligt direktiv (EU) 2015/2366 (andra betaltjänstdirektivet) (EBA/GL/2017/10)

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 normala betalningstransaktioner som utförs genom de berörda betaltjänsterna.

ii. Berörda betaltjänstanvändare

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

iii. Säkerhetsöverträdelse avseende nätverk eller informationssystem

Betaltjänstleverantörer ska fastställa om en illasinnad handling har äventyrat nätverkets eller informationssystemets säkerhet i samband med betaltjänsternas tillhandahållande.

iv. 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 betaltjänstoperatören.

v. Ekonomiska effekter

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

vi. Hög intern upptrappningsnivå

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

vii. 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.

viii. 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) eller där en korrekt betalning på annat sätt har förhindrats eller motverkats genom incidenten.

Vid operativa incidenter som påverkar förmågan att initiera och/eller genomföra transaktioner ska betaltjänstleverantörer endast anmäla de incidenter som pågår under längre tid än en timme. Incidentens varaktighet bör mätas från det att den uppstår till dess att ordinarie verksamhet har återställts till den servicenivå som gällde innan incidenten inträffade.

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).

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.

Vid operativa incidenter som påverkar förmågan att initiera och/eller genomföra transaktioner ska betaltjänstleverantörer endast anmäla de incidenter som pågår under längre tid än en timme. Incidentens varaktighet bör mätas från det att den uppstår till dess att ordinarie verksamhet har återställts till den servicenivå som gällde innan incidenten inträffade.

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. Säkerhetsöverträdelse avseende nätverk eller informationssystem

Betaltjänstleverantörer ska fastställa om en illasinnad handling har äventyrat nätverkets eller informationssystemets säkerhet i samband med betaltjänsternas tillhandahållande.

iv. 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.

v. 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 forensiska 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 uppkomma.

vi. *Hög intern upptrappningsnivå*

Betaltjänstleverantörer ska beakta huruvida ledningsorganet, såsom det definieras i EBA:s riktlinjer för IKT-risker och säkerhetsrisker 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/pågår, i enlighet med riktlinje 60 d i EBA:s riktlinjer för IKT-risker och säkerhetsrisker. Dessutom ska betaltjänstleverantörer beakta huruvida ett krisläge har utlösts eller sannolikt kommer att utlösas på grund av incidentens påverkan på betalningsrelaterade tjänster.

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

Betaltjänstleverantörer ska bedöma incidentens påverkan på den finansiella marknaden, vilken ska tolkas som infrastrukturer och/eller betalningssystem 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.

viii. *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) betaltjänstanvändare och/ eller andra betaltjänstleverantörer har klagat på incidentens negativa effekter, ii) incidenten har påverkat en synlig betaltjänstrelaterad process och därför sannolikt kommer att uppmärksammas eller redan har uppmärksammats i medier (inte endast med beaktande av traditionella medier, såsom tidningar, utan även bloggar, sociala nätverk etc.), iii) avtalsförpliktelser har åsidosatts eller sannolikt kommer att åsidosättas med följden att rättsliga åtgärder inleds mot betaltjänstleverantören, iv) lagstadgade krav har åsidosatts och ger anledning till tillsynsåtgärder eller sanktioner som

har gjorts eller sannolikt kommer att göras offentligt tillgängliga och v) 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** incidentens varaktighet > 1 timme* **eller** > 500 000 euro **och** incidentens varaktighet > 1 timme*	> 25% av betaltjänstleverantörens normala transaktionsnivå (vad gäller antalet transaktioner) **eller** > 15 000 000 euro
Berörda betaltjänstanvändare	> 5 000 **och** incidentens varaktighet > 1 timme* **eller** > 10 % av betaltjänstleverantörens betaltjänstanvändare **och** incidentens varaktighet > 1 timme*	> 50 000 **eller** > 25 % av betaltjänstleverantörens betaltjänstanvändare
Driftavbrott	> 2 timmar	Ej tillämpligt
Säkerhetsöverträdelse avseende nätverk eller informationssystem	Ja	Ej tillämpligt
Ekonomiska effekter	Ej tillämpligt	> Max (0,1 % primärkapital**, 200 000 euro) **eller** > 5 000 000 euro
Hög intern upptrappningsnivå	Ja	Ja, och krisläge (eller motsvarande) kommer sannolikt att utlysas
Andra betaltjänstleverantörer eller relevanta infrastrukturer kan beröras	Ja	Ej tillämpligt
Effekter på anseendet	Ja	Ej tillämpligt

* Tröskelvärdet för incidenter vars varaktighet överskrider en timme tillämpas endast på operativa incidenter som påverkar betaltjänstleverantörens förmåga att initiera och/eller genomföra transaktioner.

**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 nedåt (från allvarlig till mindre allvarlig). Omklassificering av incidenter från allvarliga till mindre allvarliga ska utan onödigt dröjsmål rapporteras till den behöriga myndigheten i enlighet med riktlinje 2.21.

Riktlinje 2: Anmälningsförfarande

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

2.2. Betaltjänstleverantörer ska använda samma mall vid inlämnandet av inledande, mellanliggande och slutliga rapporter gällande samma incident. Betaltjänstleverantörer ska därför fylla i mallen etappvis och i tillämpliga fall uppdatera informationen från tidigare rapporter.

2.3. Betaltjänstleverantörer ska i tillämpliga fall även till den behöriga myndigheten i hemmedlemsstaten lämna en kopia av den information som har tillhandahållits (eller kommer att tillhandahållas) till deras användare, utan onödigt dröjsmål, i enlighet med andra stycket i artikel 96.1 i andra betaltjänstdirektivet.

2.4. Betaltjänstleverantörer ska på begäran av den behöriga myndigheten i hemmedlemsstaten tillhandahålla ytterligare dokument som kompletterar informationen som lämnats i standardmallen. 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.

2.5. Eventuell kompletterande information i dokumenten som betaltjänstleverantören tillhandahåller till den behöriga myndigheten, antingen på initiativ av betaltjänstleverantören eller på begäran av den behöriga myndigheten i enlighet med riktlinje 2.4, ska av betaltjänstleverantören anges i mallen enligt riktlinje 2.1.

2.6. Betaltjänstleverantörer ska alltid säkerställa konfidentialiteten och integriteten när det gäller den information som utväxlas med den behöriga myndigheten i deras hemmedlemsstat, samt korrekt autentisering i förhållande till den behöriga myndigheten i hemmedlemsstaten.

Inledande rapport

2.7. Betaltjänstleverantörer ska inge en inledande rapport till den behöriga myndigheten i hemmedlemsstaten när en operativ incident eller en säkerhetsincident klassificerats som allvarlig. De behöriga myndigheterna bör utan onödigt dröjsmål bekräfta mottagandet av den inledande rapporten och tilldela den ett unikt referensnummer som otvetydigt identifierar incidenten. Betaltjänstleverantörer ska ange referensnumret vid uppdateringar av den inledande, mellanliggande eller slutliga rapporten för en och samma incident, såvida inte den mellanliggande och den slutliga rapporten lämnas in tillsammans med den inledande rapporten.

2.8. Betaltjänstleverantörer ska skicka den inledande rapporten till den behöriga myndigheten inom fyra timmar från den tidpunkt då den operativa eller säkerhetsincidenten klassificeras som allvarlig. Om det är ett känt att den behöriga myndighetens rapporteringskanaler inte är tillgängliga eller inte är i funktion vid tidpunkten i fråga, ska betaltjänstleverantörer skicka den inledande rapporten så snart som de är tillgängliga/i funktion igen.

2.9. Betaltjänstleverantörer ska klassificera incidenten i enlighet med riktlinjerna 1.1 och 1.4 i rätt tid efter det att incidenten upptäckts: inte senare än 24 timmar efter upptäckten och utan onödigt dröjsmål efter det att den begärda informationen för att klassificera incidenten är tillgänglig för betaltjänstleverantören. Om det behövs längre tid för att klassificera incidenten ska betaltjänstleverantörer förklara skälen till detta i den inledande rapporten som inges till den behöriga myndigheten.

2.10. Betaltjänstleverantörer ska även inge en inledande rapport till den behöriga myndigheten i hemmedlemsstaten om en incident som tidigare inte bedömts som allvarlig omklassificeras som 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.

2.11. Betaltjänstleverantörer ska i den inledande rapporten ge rubrikinformation (avsnitt A i mallen) och redovisa för incidentens huvudsakliga drag och de konsekvenser som den förväntas få, baserat på den information som fanns tillgänglig direkt efter det att den klassificerades som allvarlig. Om några faktiska uppgifter inte är tillgängliga ska betaltjänstleverantören företa uppskattningar.

Mellanliggande rapport

2.12. Betaltjänstleverantörer ska inge mellanliggande rapporter när den normala verksamheten och driften återupptagits, för att informera den behöriga myndigheten om detta. Betaltjänstleverantörer ska anse att driften är normal igen när verksamheten/driften har återgått till den servicenivå och de villkor som definierats av betaltjänstleverantören eller fastställts externt genom ett servicenivåavtal (som reglerar behandlingstider, kapacitet,

säkerhetskrav osv.) och det inte längre föreligger några beredskapsåtgärder. Den mellanliggande rapporten ska innehålla en mer detaljerad beskrivning av incidenten och dess konsekvenser (avsnitt B i mallen).

2.13. Om man ännu inte kunnat återgå till normal drift ska betaltjänstleverantörer inge en mellanliggande rapport till den behöriga myndigheten inom tre arbetsdagar från det att den inledande rapporten lämnades in.

2.14. Betaltjänstleverantörer ska uppdatera den information som redan tillhandahållits i avsnitten A och B i mallen om de får kännedom om betydande förändringar sedan den föregående rapporten ingavs (t.ex. om incidenten har förvärrats eller minskat i allvarlighetsgrad, om nya orsaker identifierats eller nya åtgärder har vidtagits för att lösa problemet). I detta ingår om incidenten inte kunnat åtgärdas under loppet av tre arbetsdagar. I detta fall utlöses ett krav på ytterligare en mellanliggande rapport från betaltjänstleverantören. Betaltjänstleverantörer ska i alla händelser upprätta en mellanliggande rapport på begäran från den behöriga myndigheten i hemmedlemsstaten.

2.15. På samma sätt som för inledande rapporter ska betaltjänstleverantörer göra uppskattningar i de fall inga faktiska uppgifter finns tillgängliga.

2.16. Om driften normaliserats inom fyra timmar från det att incidenten klassificerades som allvarlig ska betaltjänstleverantören sträva efter att inge den inledande rapporten och den 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 underliggande orsakerna har ägt rum (oberoende av huruvida skadebegränsande åtgärder redan har genomförts eller den slutgiltiga underliggandeorsaken har identifierats) och faktiska uppgifter är tillgängliga som kan ersätta eventuella uppskattningar.

2.18. Betaltjänstleverantörer ska inge slutrapporten till den behöriga myndigheten senast 20 arbetsdagar efter det att driften anses vara normal igen. Betaltjänstleverantörer som behöver en förlängd tidsfrist (t.ex. om det ännu inte finns några tillgängliga uppgifter om effekterna eller om den underliggande orsaken ännu inte har kunnat fastställas) 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 klassificerades som allvarlig, ska de sträva efter att inge all information på en gång, dvs den som krävs i den inledande rapporten, i den mellanliggande rapporten och i slutrapporten.

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

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 kriterierna för att anses allvarlig och inte antas uppfylla dem innan incidenten avhjälps. I detta fall ska betaltjänstleverantörer skicka slutrapporten så snart som denna omständighet upptäcks och under alla förhållanden senast inom tidsfristen för inlämningen av nästa rapport. I denna särskilda situation ska betaltjänstleverantören, i stället för att fylla i avsnitt C i mallen, kryssa för rutan ”incident omklassificerad som icke-allvarlig” och förklara skälen till 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 rapportering 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 utkontraktering av viktiga operativa funktioner i enlighet med

   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. EBA:s riktlinjer om utkontraktering (EBA/GL/2019/02) i med avseende på alla betaltjänstleverantörer.

c. Informationen ska inges till den behöriga myndigheten i hemmedlemsstaten på förhand och, under alla omständigheter, 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 anges 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. En för över samtliga betaltjänstleverantörer som påverkats av incidenten ska tillhandahållas.

e. Det ska säkerställas att den tredje parten bedömer incidentens allvarlighetsgrad 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.

f. Det ska vad gäller de fält i mallen där ett gemensamt svar inte är möjligt (t.ex. avsnitt B2, B4 eller C3), 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 observerade eller uppskattade kumulativa värden för betaltjänstleverantörerna.

g. Tredje part håller betaltjänstleverantören ständigt informerad 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 väsentlig 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.

3.6. Betaltjänstleverantörer ska säkerställa att, i situationen där en incident orsakas av ett avbrott i tjänster utförda av en teknisk leverantör (eller av infrastruktur) och som påverkar flera betaltjänstleverantörer, delegerad rapportering hänvisar till : individuella uppgifter (förutom vid konsoliderad rapportering).

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 definierade 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 allvarlighetsgrad:

a. Orsakerna till incidenten omfattas av den andra inhemska myndighetens tillsynsbefogenheter (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 medierna.

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, minst vid den tidpunkt när de erhåller den inledande rapporten (eller, alternativt, den rapport som föranledde delningen av information) och när de erhåller underrättelse om att verksamheten fungerar normalt igen (dvs. den mellanliggande rapporten).

6.2. Den behöriga myndigheten ska till andra relevanta inhemska myndigheter lämna den information som behövs för att tillhandahålla en klar bild av vad som har hänt och de potentiella konsekvenserna. 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 då incidenten klassificerades som allvarlig.
- Datum och tidpunkt då incidenten upptäcktes.
- Datum och tidpunkt då incidenten började.
- Datum och tidpunkt då incidenten återställdes eller förväntas bli 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 återhämtning från incidenten.
- En beskrivning av hur incidenten kan komma att påverka andra betaltjänstleverantörer och/eller infrastrukturer.
- En beskrivning av en eventuell rapportering i medierna.
- 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. Den behöriga myndigheten ska dock 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. Betaltjänstleverantörer ska alltid säkerställa konfidentialiteten och integriteten när det gäller den information som utväxlas med den behöriga myndigheten i deras hemmedlemsstat, samt korrekt autentisering i förhållande till den behöriga myndigheten i hemmedlemsstaten. 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 rapporter, mellanliggande rapporter eller slutrapporter).

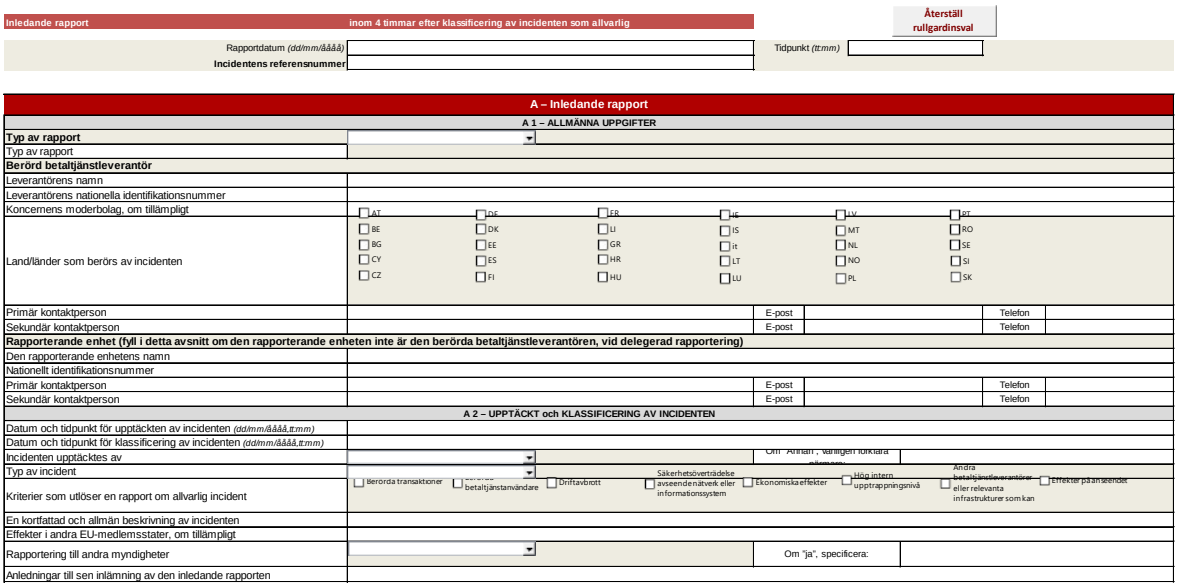
Riktlinje 8: Kommunikation

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 driftavbrott, ska behöriga myndigheter stödja lämpliga kommunikationsmedel.

Bilaga – Rapporteringsmall för betaltjänstleverantörer

Inledande rapport



Inledande rapport	inom 4 timmar efter klassificering av incidenten som allvarlig		Återställ rullgardinsval		
Rapportdatum *(dd/mm/åååå)*		Tidpunkt *(tt:mm)*			
Incidentens referensnummer					

A – Inledande rapport					
A 1 – ALLMÄNNA UPPGIFTER					
Typ av rapport					
Typ av rapport					
Berörd betaltjänstleverantör					
Leverantörens namn					
Leverantörens nationella identifikationsnummer					
Koncernens moderbolag, om tillämpligt					
Land/länder som berörs av incidenten	☐ AT ☐ BE ☐ BG ☐ CY ☐ CZ ☐ DE ☐ DK ☐ EE ☐ ES ☐ FI ☐ FR ☐ LI ☐ GR ☐ HR ☐ HU ☐ IE ☐ IS ☐ it ☐ LT ☐ LU ☐ LV ☐ MT ☐ NL ☐ NO ☐ PL ☐ PT ☐ RO ☐ SE ☐ SI ☐ SK				
Primär kontaktperson		E-post		Telefon	
Sekundär kontaktperson		E-post		Telefon	
Rapporterande enhet (fyll i detta avsnitt om den rapporterande enheten inte är den berörda betaltjänstleverantören, vid delegerad rapportering)					
Den rapporterande enhetens namn					
Nationellt identifikationsnummer					
Primär kontaktperson		E-post		Telefon	
Sekundär kontaktperson		E-post		Telefon	
A 2 – UPPTÄCKT och KLASSIFICERING AV INCIDENTEN					
Datum och tidpunkt för upptäckten av incidenten *(dd/mm/åååå,tt:mm)*					
Datum och tidpunkt för klassificering av incidenten *(dd/mm/åååå,tt:mm)*					
Incidenten upptäcktes av		Om "Annan", vänligen förklara närmare:			
Typ av incident					
Kriterier som utlöser en rapport om allvarlig incident	☐ Berörda transaktioner ☐ [illegible] betaltjänstanvändare ☐ Driftavbrott ☐ Säkerhetsöverträdelse avseende nätverk eller informationssystem ☐ Ekonomiska effekter ☐ Hög intern upptrappningsnivå ☐ Andra betaltjänstleverantörer eller relevanta infrastrukturer som kan ☐ Effekter på anseende				
En kortfattad och allmän beskrivning av incidenten					
Effekter i andra EU-medlemsstater, om tillämpligt					
Rapportering till andra myndigheter		Om "ja", specificera:			
Anledningar till sen inlämning av den inledande rapporten					

Mellanliggande rapport

Rapport om allvarliga incidenter

Mellanliggande rapport	inte senare än inom tre arbetsdagar från inlämnandet av den inledande rapporten	Återställ rullgardinsval

Rapportdatum *(dd/mm/åååå)* | Tidpunkt *(tt:mm)*

Incidentens referensnummer

B – Mellanliggande rapport

B 1 – ALLMÄNNA UPPGIFTER

Mer detaljerad beskrivning av incidenten:	
Vad är det specifika problemet?	
Hur började incidenten?	
Hur utvecklades den?	
Vilka är konsekvenserna (i synnerhet för betaltjänstanvändare)?	
Informerades betaltjänstanvändare om incidenten?	Om "ja", specificera:
Var den relaterad till tidigare incident/incidenter?	Om "ja", specificera:
Var andra tjänsteleverantörer/tredje parter påverkade eller involverade?	Om "ja", specificera:
Påbörjades krishanteringen (intern och/eller extern)?	Om "ja", specificera:
Datum och tidpunkt för incidentens början (om denna redan är identifierad) *(dd/mm/åååå, tt:mm)*	
Datum och tidpunkt då incidenten återställdes eller förväntas bli återställd *(dd/mm/åååå, tt:mm)*	
Berörda funktionsområden	☐ Autentisering/auktorisation ☐ Direkt avveckling ☐ Kommunikation ☐ Indirekt avveckling ☐ Clearing ☐ Övrigt — Om "Övrigt", vänligen spec
Ändringar som gjorts i tidigare rapporter	

B 2 – KLASSIFICERING/INFORMATION OM INCIDENTEN

Berörda transaktioner [2]	Effektnivån Antal berörda transaktioner Som en procentandel av normalt antal transaktioner Värde av de berörda transaktionerna i euro Incidentens varaktighet (endast tillämpligt för operativa incidenter) Kommentarer:
Berörda betaltjänstanvändare [3]	Effektnivån Antal berörda betaltjänstanvändare Som en procentandel av de sammanlagda betaltjänstanvän
Säkerhetsöverträdelse avseende nätverk eller informationssystem	Beskriv hur nätverket eller informationssystemen har påverkats
Driftavbrott	Totalt tid för driftavbrott — Dagar: — Timmar: — Minuter:
Ekonomiska effekter	Effektnivån Direkta kostnader i euro Indirekta kostnader i euro
Hög intern upptrappningsnivå	Beskriv den interna upptrappningsnivån för incidenten och ange om den har utlöst eller sannolikt kommer att utlösa ett krisläge (eller motsvarande). Om detta är fallet, vänligen lämna en beskrivning
Andra betaltjänstleverantörer eller relevanta infrastrukturer som kan beröras	Beskriv hur incidenten kan påverka andra betaltjänstleverantörer och/eller infrastrukturer
Effekter på anseendet	Beskriv hur incidenten kan påverka betaltjänstleverantörens anseende (t.ex. rapportering i medier, offentliggörande av rättsliga åtgärder eller lagöverträdelser, etc.)

B 3 – BESKRIVNING AV INCIDENTEN

Typ av incident	
Orsaken till incidenten	☐ Under utredning ☐ Illasinnad handling ☐ Processfel ☐ Systemfel ☐ Mänskligt misstag ☐ Externa händelser ☐ Övrigt — Om "Övrigt", vänligen specificera:
Påverkade incidenten er direkt eller påverkades ni indirekt genom en tjänsteleverantör?	Om indirekt, vänligen ange tjänsteleverantörens namn:

B 4 – INCIDENTENS EFFEKTER

Sammanlagd effekt	☐ Integritet ☐ Konfidentialitet ☐ Tillgänglighet ☐ Autenticitet
Berörda kommersiella kanaler	☐ Filialer ☐ Telefonbanktjänster ☐ Försäljningsställe ☐ Internetbanktjänster ☐ Mobila banktjänster ☐ Övrigt ☐ E-handel ☐ Uttagsautomater Om "Övrigt", vänligen specificera:
Berörda betaltjänster	☐ Kontantinsättning på ett betalkonto ☐ Kreditöverföringar ☐ Penningöverföring ☐ Kontantuttag från ett betalkonto ☐ Autogireringar ☐ Betalningsinitiering ☐ Transaktioner som krävs för att förvalta ett betalkonto ☐ Kortbetalningar ☐ Kontoinformationstjänster ☐ Förvärv av betalningsinstrument ☐ Utfärdande av betalningsinstrument

B 5 – BEGRÄNSNING AV INCIDENTEN

Vilka handlingar/åtgärder har vidtagits hittills eller är planerade för återhämtning från incidenten?	
Har kontinuitetsplanen och/eller katastrofplanen aktiverats?	
Om "ja", när? *(dd/mm/åååå, tt:mm)*	
Om "ja", beskriv närmare	

Slutrapport

Rapport om allvarlig incident

Välj typ av rapport:

Vänligen beskriv: (tillämpligt för incidenter klassificerade som mindre allvarliga)

inom 20 dagar från tidpunkten för inlämnandet av den mellanliggande rapporten

Återställ rullgardinsval

Rapportdatum *(dd/mm/åååå)*: Tidpunkt *(tt:mm)*:

Incidentens referensnummer:

C – Slutrapport

Om ingen mellanliggande rapport har ingetts, var god fyll även i avsnitt B

C 1 – ALLMÄNNA UPPGIFTER

Uppdatering av informationen i den inledande och den mellanliggande rapporten	
Ändringar som gjorts i tidigare rapporter	
Annan relevant information	
Är alla ursprungliga kontroller på plats? Om svaret är nej, ange vilka kontroller det gäller och hur lång period som behövs för att återställa dem.	

C 2 – ANALYS AV DE UNDERLIGGANDE ORSAKERNA OCH UPPFÖLJNING

Vilken var den underliggande orsaken (om den är känd)?

☐ Illvillig handling ☐ Processfel ☐ Systemfel ☐ Mänskligt misstag ☐ Externa händelser ☐ Annat

Precisera:

Illvillig handling	Processfel	Systemfel	Mänskligt misstag	Externa händelser
Skadlig kod	Bristande övervakning och kontroll	Maskinvarufel	Oavsiktlig	Fel från en leverantörs eller en teknisk tjänsteleverantörs sida
Insamling av information	Kommunikationsproblem	Nätverksfel	Avsaknad av	
Intrång	Olämplig verksamhet	Databasproblem	Otillräckliga resurser	Force majeure
Överbelastningsattack (D/DoS)	Otillräcklig ändringshantering	Fel i mjukvaran/applikationen	Annat	Annat
Avsiktliga interna handlingar	Otillräckliga interna förfaranden och otillräcklig dokumentation	Fysiska skador		
Avsiktlig extern fysisk skadegörelse	Återställningsproblem	Annat		
Informationsinnehållssäkerhet	Annat			
Bedrägliga				
Övrigt				

Om "Övrigt", vänligen specificera:

Annan relevant information om den grundläggande orsaken	
Huvudsakliga korrigerande åtgärder/åtgärder som vidtagits eller planeras för att förhindra att incidenten inträffar igen i framtiden, om de redan är kända	

C 3 – YTTERLIGARE INFORMATION

Har andra betaltjänstleverantörer informerats om incidenten?	Om ja, ange detaljer:
Har någon rättslig åtgärd vidtagits mot betaltjänstleverantören?	Om ja, ange detaljer:
Bedömning av effektiviteten hos de åtgärder som vidtagits	Ange detaljer:

INSTRUKTIONER FÖR IFYLLANDE AV MALLEN

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 den mellanliggande rapporten och avsnitt C för slutrapporten. Betaltjänstleverantörer ska använda samma mall när de lämnar in den inledande rapporten, den mellanliggande rapporten och slutrapporten om dessa gäller en och samma incident. Alla fält är obligatoriska såvida inte något annat uttryckligen anges.

Rubrik

Inledande rapport: Detta är den första anmälan som betaltjänstleverantören lämnar in till den behöriga myndigheten i hemmedlemsstaten.

Mellanrapport: Denna rapport innehåller en mer detaljerad beskrivning av incidenten och dess konsekvenser. Det är en uppdatering av den inledande rapporten (och, om tillämpligt, av en tidigare mellanliggande rapport) gällande samma incident.

Slutrapport: Detta är den slutgiltiga rapporten som betaltjänstleverantören kommer att skicka in om incidenten, eftersom i) en analys av de underliggande orsakerna redan har genomförts och uppskattningarna kan ersättas med faktiska siffror eller ii) incidenten inte längre anses vara allvarlig och behöver omklassificeras.

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

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

Incidentens identifikationsnummer (för mellanliggande rapporter, slutrapporter och uppdateringar av inledande rapporter): Det referensnummer som den behöriga myndigheten har utfärdat vid tidpunkten för den inledande rapporten för en unik identifiering av incidenten. Den behöriga myndigheten ska lägga till den tvåsiffriga ISO-landskoden[2] för medlemsstaten som prefix.

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 inom samma medlemsstat som påverkas av samma allvarliga operativa eller säkerhetsincident och därför 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.

Betaltjänstleverantörens namn: Det fullständiga namnet på den betaltjänstleverantör som är föremål för rapporteringsförfarandet såsom det anges i det tillämpliga officiella nationella registret över betaltjänstleverantörer.

Betaltjänstleverantörens identifikationsnummer: Ett unikt nationellt identifikationsnummer som används av den behöriga myndigheten i hemmedlemsstatens nationella register för att på ett otvetydigt sätt identifiera betaltjänstleverantören.

Koncernens moderbolag: Om det rör sig om en koncern enligt definitionen i artikel 4.40 i andra betaltjänstdirektivet, ange namnet på moderbolaget.

[2] För mer information, se alpha-2-landskoderna enligt standarden ISO-3166 på https://www.iso.org/iso-3166-country-codes.html

Land/länder där incidenten har haft påverkan: Land eller länder för vilka incidenten har fått konsekvenser (till exempel om en betaltjänstleverantörs filialer i olika länder har påverkats), oberoende av incidentens allvarlighetsgrad i övriga länder. Detta kan men behöver inte vara samma land 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/riskhantering eller liknande område vid den berörda betaltjänstleverantören.

E-post: E-postadress till vilken förfrågningar om ytterligare klargöranden kan skickas vid behov. Det kan antingen vara en personlig e-postadress eller en företagsadress.

Telefonnummer: Telefonnummer för förfrågningar om ytterligare klargöranden, vid behov. Det kan vara ett personligt telefonnummer eller ett företagsnummer.

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

E-post: E-postadress till den alternativa kontaktperson som vid behov kan kontaktas för ytterligare klargöranden. Det kan vara en personlig e-postadress eller en företagsadress.

Telefon: Telefonnummer till den alternativa kontaktperson som vid behov kan kontaktas för ytterligare klargöranden. Det kan vara ett personligt telefonnummer eller ett företagsnummer.

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

Namn på den rapporterande enheten: Fullständigt namn på den enhet som rapporterar incidenten såsom det anges i det tillämpliga officiella nationella företagsregistret.

Nationellt identifikationsnummer: Ett unikt nationellt identifikationsnummer som används i det land där den tredje parten har sitt säte för att entydigt identifiera enheten som rapporterar om incidenten. Om den rapporterande tredje parten är en betaltjänstleverantör ska det nationella identifikationsnumret ska vara det unika nationella identifikationsnummer som används av den behöriga myndigheten för att identifiera betaltjänstleverantören i fråga i hemmedlemsstaten och i dess nationella register.

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

E-post: E-postadress som kan användas för förfrågningar om ytterligare klargöranden, vid behov. Det kan vara en personlig e-postadress eller en företagsadress.

Telefonnummer: Telefonnummer för förfrågningar om ytterligare klargöranden, vid behov. Det kan vara ett personligt telefonnummer eller ett företagsnummer.

Sekundär kontaktperson: Förnamn och efternamn på en alternativ kontaktperson från enheten som rapporterar incidenten, som den behöriga myndigheten kan kontakta om den primära kontaktpersonen inte skulle vara tillgänglig.

E-post: E-postadress till den alternativa kontaktperson som vid behov kan kontaktas för ytterligare klargöranden. Det kan vara en personlig e-postadress eller en företagsadress.

Telefon: Telefonnummer till den alternativa kontaktperson som vid behov kan kontaktas för ytterligare klargöranden. Det kan vara ett personligt telefonnummer eller ett företagsnummer.

A 2 - Upptäckt och klassificering av en incident

Datum och tid då incidenten upptäcktes: Datum och tid då incidenten identifierades första gången.

Datum och tidpunkt för klassificeringen av incidenten: Datum och tidpunkt då säkerhetsincidenten eller den operativa incidenten klassificerades som allvarlig.

Incidenten upptäcktes av: Ange huruvida incidenten upptäcktes av en betaltjänstanvändare, av betaltjänstleverantören (t.ex. tjänsten för internrevision) eller en extern part (t.ex. en tjänsteleverantör). Om incidenten inte upptäcktes av någon av dessa, ge en förklaring i motsvarande fält.

Typ av incident: I den utsträckning ni kan bedöma detta och om informationen finns tillgänglig, ange huruvida det 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 och/eller autenticitet.
>
> **Säkerhet:** Icke auktoriserad tillgång, användning, offentliggörande, störning, ändring eller förstörelse av betaltjänstleverantörens tillgångar som påverkar de betaltjänstrelaterade tjänsternas integritet, tillgänglighet, konfidentialitet och/eller autenticitet. Detta kan bland annat inträffa om betaltjänstleverantören råkar ut för säkerhetsöverträdelser avseende nätverk eller informationssystem.

Kriterier som utlöser användning av rapporten av en allvarlig incident: Ange vilket/vilka av kriterierna som har utlöst den allvarliga incidenten. Flera av kriterierna kan väljas: påverkan på transaktioner, påverkan på betaltjänstanvändare, driftavbrott, säkerhetsöverträdelser avseende nätverk eller informationssystem, ekonomiska effekter, hög intern upptrappningsnivå, andra betaltjänstleverantörer eller relevanta infrastrukturer kan komma att påverkas och/eller påverkan på anseendet.

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

Påverkan i andra EU-medlemsstater, om tillämpligt: Redogör kortfattat för vilken påverkan incidenten haft i andra EU-medlemsstater (dvs. på betaltjänstanvändare, betaltjänstleverantörer och/eller betalningsinfrastrukturer). Om det är möjligt med tanke på tidsfristerna för rapportering, vänligen tillhandahåll en översättning till engelska.

Rapportering till andra myndigheter: Om det är känt vid tidpunkten för rapportering, ange om incidenten har rapporterats eller ska rapporteras till andra myndigheter inom ramen för andra rapporteringssystem. Om det är känt, ange vilken/vilka myndigheter det gäller.

Orsaker till försenad inlämning av den inledande rapporten: Förklara varför det tog mer än 24 timmar att klassificera incidenten.

B Mellanliggande rapport

B 1 – Allmänna uppgifter

Mer detaljerad beskrivning av incidenten: Beskriv incidentens huvuddrag, åtminstone vilket specifikt problem betaltjänstleverantören står inför samt tillhörande bakgrund, hur incidenten uppkom och utvecklades, dess konsekvenser, särskilt för betaltjänstanvändare, osv. Tillhandahåll även information om kommunikationen med betaltjänstanvändarna, i förekommande fall.

Kopplingar till tidigare incidenter: Ange om incidenten har koppling till tidigare incidenter, om den informationen är tillgänglig. Om incidenten har koppling till tidigare incidenter, specificera vilken/vilka.

Påverkades eller involverades andra tjänsteleverantörer/tredje parter? Om informationen är tillgänglig, ange om incidenten har påverkat eller inbegripit andra tjänsteleverantörer eller tredje parter. Om incidenten har påverkat eller involverat andra tjänsteleverantörer eller tredje parter, ange vilka de är och ge mer information.

Har krishanteringsförfaranden (interna och/eller externa) utlösts? Ange om krishanteringsförfaranden (interna och/eller externa) har utlösts. Om krishanteringen har påbörjats, lämna mer information.

Datum och tidpunkt då incidenten uppstod: Datum och tidpunkt då incidenten uppstod, om detta är känt.

Datum och tidpunkt för när incidenten återställdes eller förväntas bli återställd: Ange datum och tidpunkt för när incidenten var eller förväntas vara under kontroll och när verksamheten återgick eller förväntas återgå till det normala igen.

Berörda funktionsområden: Ange det eller de steg i betalningsprocessen som incidenten har påverkat, till exempel autentisering/auktorisation, kommunikation, clearing, direkt avveckling eller indirekt avveckling.

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.

Kommunikation: Informationsflöde som används för identifiering, autentisering, meddelanden och information mellan kontoförvaltande betaltjänstleverantörer 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 slutliga 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.

Ändringar gjorda i tidigare rapporter: Ange vilka ändringar som gjorts i förhållande till information som rapporterats genom tidigare rapporter om samma incident (dvs. den inledande eller, om tillämpligt, den mellanliggande rapporten).

B 2 – Klassificering av incidenten/information om incidenten

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 konkreta värden för dessa variabler, vilka antingen kan utgöra faktiska siffror eller uppskattningar. 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 fältet ”Kommentarer”. I de fall där transaktioner i andra valutor än euro påverkats av incidenten ska betaltjänstleverantörerna vid beräkning av trösklar och rapportering av värdet av de påverkade transaktionerna omvandla

summan av transaktionerna som gjorts i andra valutor än euro till euro med hjälp av ECB:s dagliga referensväxelkurs för dagen före inlämnandet av incidentrapporten.

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. 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 (i förekommande fall) och de betaltjänstleverantörer som tar emot dessa operativa tjänster ska också dem 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.

Säkerhetsöverträdelse avseende nätverk eller informationssystem: Betaltjänstleverantörer ska avgöra om någon illasinnad handling har äventyrat tillgängligheten, autenticiteten, integriteten eller konfidentialiteten avseende nätverk eller informationssystem (inklusive data) med koppling till tillhandahållandet av betaltjänsterna.

Driftavbrott: Betaltjänstleverantörer ska ange om tröskeln har uppnåtts eller sannolikt kommer att uppnås genom incidenten och den relaterade siffran: total tid för driftavbrott. Betaltjänstleverantörer ska tillhandahålla konkreta värden för denna variabel, vilka antingen kan utgöra faktiska siffror eller uppskattningar. 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 då det uppkommer och beakta såväl tidsintervaller när de är öppna för handel så som krävs för genomförandet av betaltjänster, som intervaller när de är stängda samt underhållsperioder, om det är relevant och tillämpligt. Om betaltjänstleverantörer inte kan fastställa när driftavbrottet inträffade ska de undantagsvis beräkna driftavbrottet från den tidpunkt då 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. 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 forensiska kostnader eller kostnader för avhjälpande, avgifter på grund av åsidosättande av avtalsförpliktelser, sanktioner, externa skulder och förlorade intäkter. Vad gäller indirekta kostnader ska betaltjänstleverantörer endast beakta kostnader som redan är kända eller med stor sannolikhet kommer att uppstå. I de fall där kostnaderna är i andra valutor än euro ska betaltjänstleverantörerna vid beräkning av trösklar och rapportering av den ekonomiska effekten omvandla summan av kostnaderna i andra valutor än euro till euro med hjälp av ECB:s dagliga referensväxelkurs för dagen före inlämnandet av incidentrapporten.

Direkta kostnader: Kostnader (i euro) som uppstått direkt till följd 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: Kostnader (i euro) som uppstått indirekt till följd av incidenten (dvs. reklamationer/kompensationskostnader, eventuella rättegångskostnader).

Hög intern upptrappningsnivå: Betaltjänstleverantörer ska beakta huruvida ledningsorganet, såsom det definieras i EBA:s riktlinjer för IKT-risker och säkerhetsrisker, 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/pågår, i enlighet med riktlinje 60 d i EBA:s riktlinjer för IKT-risker och säkerhetsrisker. Dessutom ska betaltjänstleverantörer beakta huruvida ett krisläge har utlösts eller sannolikt kommer att utlösas på grund 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 stor exponering incidenten, i den mån de har kännedom om detta, har fått eller sannolikt kommer att få 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) betaltjänstanvändare och/ eller andra betaltjänstleverantörer har klagat på incidentens negativa effekter, ii) incidenten har påverkat en synlig betaltjänstrelaterad process och därför sannolikt kommer att uppmärksammas eller redan har uppmärksammats i medier (inte endast med beaktande av traditionella medier, såsom tidningar, utan även bloggar, sociala nätverk etc.; dock gäller att uppmärksamheten i medier av detta slag inte endast får utgöras av ett fåtal negativa kommentarer av följare, utan det ska finnas en giltig rapport eller ett betydande antal negativa kommentarer/varningar), iii) avtalsförpliktelser har åsidosatts eller sannolikt kommer att åsidosättas med följden att rättsliga åtgärder inleds mot betaltjänstleverantören, iv) lagstadgade krav har åsidosatts och ger anledning till tillsynsåtgärder eller sanktioner som har gjorts eller sannolikt kommer att göras offentligt tillgängliga och v) samma typ av incident har inträffat tidigare.

B 3 – Beskrivning av incidenten

Typ av incident: operativ incident eller säkerhetsincident. En kompletterande förklaring finns i motsvarande fält i den inledande rapporten.

Orsak till incidenten: Ange vad som orsakat incidenten. Om detta inte är känd ännu, ange den mest sannolika orsaken. Flera alternativ kan väljas.

Under utredning Markera kryssrutan om orsaken för närvarande är okänd.

Skadlig handling: Illasinnade handlingar riktade direkt mot betaltjänstleverantören i fråga. Dessa kan innefatta skadlig kod, samlande av information, intrång, samordnade överbelastningsattacker (D/DoS), avsiktliga interna åtgärder, avsiktliga externa fysiska skador,

informationsinnehållssäkerhet, bedrägliga operationer osv. För mer information, se avsnitt C2 i denna mall.

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

Systemfel: Orsaken till incidenten är kopplad till brister i frågan om design, genomförande, komponenter, specifikationer, integration eller komplexitet hos de system som stödjer betalningsoperationen.

Mänskligt fel: Incidenten orsakades av en persons oavsiktliga misstag, antingen som en del av betalningsförfarandet (t.ex. uppladdning av fel kommandofil för betalningar i betalningssystemet) eller på något sätt kopplat till detta (t.ex. om strömmen bryts av en olyckshändelse så att betalningsoperationen pausas).

Externa händelser: Orsaken är kopplad till händelser som generellt sett är utanför organisationens kontroll (t.ex. naturkatastrofer eller ett fel från en teknisk tjänsteleverantör).

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

Påverkade incidenten dig direkt eller indirekt genom en tjänsteleverantör? Om informationen finns tillgänglig, ange om incidenten var riktad direkt mot betaltjänstleverantören eller om den påverkar den indirekt via en tredje part. Om svaret är indirekt påverkan, ange namnet på tjänsteleverantören/leverantörerna.

B 4 – Effekter av incidenten

Sammanlagd effekt: Ange vilka aspekter som påverkats av den operativa incidenten eller säkerhetsincidenten. Flera alternativ kan väljas.

Integritet: Säkerställande av att tillgångarna (inbegripet data) är korrekta och fullständiga.

Tillgänglighet: Betaltjänsterna är fullt tillgängliga och kan användas av betaltjänstanvändare, enligt godkända fördefinierade nivåer.

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.

Berörda kommersiella kanaler: Ange den kanal/de kanaler som används för interaktion med de betaltjänstanvändare som berörts av incidenten. Flera rutor kan markeras.

Filial: Ett driftsställe (annat än huvudkontoret) som utgör en del av en betaltjänstleverantör, men som inte är en juridisk person och som genomför alla eller vissa av de transaktioner som hänför sig till betaltjänstleverantörens verksamhet. Alla driftsställen som inrättats i en och 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 hjälp av datorer.

Telefonbanktjänster: Genomförande av finansiella transaktioner med via telefon.

Mobila banktjänster: Genomförande av finansiella transaktioner med användning av en särskild bankapp på en smarttelefon eller liknande enhet.

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

Försäljningsställe: Näringsidkarens fysiska lokaler, där betaltransaktioner initieras.

E-handel: Betalningstransaktionen inleds på ett virtuellt försäljningsställe (t.ex. betalningar som görs via internet med hjälp av kreditöverföringar, betalkort, överföring av elektroniska pengar mellan konton för elektronisk valuta).

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 kan markeras.

Kontantinsättning på ett betalkonto: Inlämning av kontanter till en betaltjänstleverantör för insättning på ett betalkonto.

Kontantuttag från ett betalkonto: En begäran som en betaltjänstleverantör erhåller från dess betaltjänstanvändare om att tillhandahålla kontanter och debitera användarens betalkonto med motsvarande belopp.

Transaktioner som krävs för att förvalta ett betalkonto: De operationer som behöver göras på ett betalkonto 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.

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

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

Kortbetalning: En betaltjänst som grundas på kontokortsystemets infrastruktur och verksamhetsregler 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 betaltjänst på nätet som tillhandahåller sammanställd information om ett eller flera betalkonton som betaltjänstanvändaren antingen innehar hos en annan betaltjänstleverantör eller hos fler än en betaltjänstleverantör.

B 5 – Begränsning av incidenten

Vilka åtgärder har hittills vidtagits eller är planerade för återhämtning efter incidenten? Ange detaljer angående de åtgärder som vidtagits eller planeras för att temporärt hantera incidenten.

Har kontinuitetsplaner och/eller katastrofplaner aktiverats? Ange om detta är fallet och tillhandahåll i förekommande fall de mest relevanta uppgifterna om vad som hänt (dvs. när planen aktiverades och vilka åtgärder som ingick i den).

C – Slutrapport

C 1 – Allmänna uppgifter

Uppdatering av informationen i den inledande rapporten och den mellanliggande rapporten/rapporterna (sammanfattning): Ge ytterligare information om incidenten, inklusive de specifika ändringar som gjorts i den mellanliggande rapporten. Inkludera även eventuell annan relevant information.

Är alla ursprungliga kontroller på plats? Ange om betaltjänstleverantören var tvungen att dra in eller försvaga några kontroller under den tid som incidenten pågick. Om svaret är ”ja”, ange om alla kontroller är på plats igen. Om så inte är fallet, använd fritextfältet för att ange vilka kontroller som ännu inte är på plats och hur lång ytterligare tid det kommer att krävas för att återställa dessa.

C 2 – Analys av de underliggande orsakerna och uppföljning

Vilken var den underliggande orsaken (om den är känd)? Ange den underliggande orsaken till incidenten eller, om den inte är känd, vad som bedöms vara den troligaste orsaken. Flera alternativ kan väljas. (Observera att åtskillnad måste göras mellan den underliggande orsaken och incidentens effekter.)

Illvillig handling: Externa eller interna handlingar avsiktligt riktade (med ont uppsåt) mot betaltjänstleverantören. Dessa delas in i följande kategorier:

Skadlig kod, t.ex. virus, internetmaskar, trojaner eller spionprogram.

Informationsuppfångning, t.ex. genom skanning, sniffing-programvara och social manipulation.

Intrång, t.ex. intrång i privilegierade konton eller oprivilegierade konton, äventyrande av applikationer, bottar.

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

Avsiktliga interna handlingar såsom sabotage eller stöld.

Avsiktlig extern fysisk skadogörelse, t.ex. sabotage, fysiska attacker mot lokaler/datacentraler.

Säkerhet avseende informationsinnehåll: Icke auktoriserad tillgång till information, icke auktoriserad modifiering av information.

Bedrägliga handlingar: Otillåten användning av resurser, rättigheter, uppträdande under falsk identitet, nätfiske.

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

Processfel: Orsaken till incidenten var bristfällig design eller ett bristfälligt genomförande av betalningsprocessen, processregleringssystemet och/eller stödjande processer (t.ex. förändring/migrering, testning, konfigurering, kapacitet, övervakning). Dessa delas in i följande kategorier:

Bristande övervakning och kontroll, t.ex. inom ramen för den löpande verksamheten, sista giltighetsdagar för certifikat och licenser, förfallodatum för uppdateringar, definierade maximala motvärden, fyllnadsnivåer för databaser, hantering av användarrättigheter, principen om dubbelkontroll.

Kommunikationsproblem, t.ex. mellan marknadsaktörer eller inom organisationen.

Olämplig verksamhet t.ex. uteblivet utbyte av certifikat, fullt cacheminne.

Otillräcklig förändringshantering, t.ex. oidentifierade konfigurationsfel, utrullningar inklusive uppgraderingar, underhållsfrågor, oväntade fel.

Otillräckliga interna förfaranden och otillräcklig dokumentation, t.ex. brist på transparens vad gäller funktioner, processer och förekomsten av funktionsstörningar, avsaknad av dokumentation.

Återställningsproblem, t.ex. i fråga om beredskapshantering, otillräcklig reservkapacitet.
Annat (specificera): Orsaken till incidenten är inte något av ovanstående. Ytterligare uppgifter ska tillhandahållas i fritextfältet.

Systemfel: Orsaken till incidenten är kopplad till brister i fråga om design, genomförande, komponenter, specifikationer, integrering eller komplexitet hos de system som stödjer betalningsoperationen. Dessa delas in i följande kategorier:

Maskinvarufel: Fel i den fysiska tekniska utrustningen i vilka processerna körs och/eller i vilka de data lagras som betaltjänstleverantörer behöver för att utföra betalningsrelaterad verksamhet (t.ex. hårddiskfel, datacentraler, annan infrastruktur).
Nätverksfel: Fel i de offentliga eller privata telekommunikationsnätverk som möjliggör utbyte av data och information (t.ex. internet) under betalningsprocessen.
Databasproblem: Problem avseende den datastruktur som lagrar personlig information och sådan betalningsrelaterad information som behövs för att genomföra betalningstransaktioner.
Programvarufel/applikationsfel: Fel i program, operativsystem osv. som stödjer tillhandahållandet av betaltjänstleverantörens betaltjänster (t.ex. funktionsstörningar, okända funktioner).
Fysisk skada:, t.ex. oavsiktlig skada orsakad av olämpliga förhållanden, byggarbeten.
Annat (precisera): Orsaken till incidenten är inte något av ovanstående. Ytterligare uppgifter ska tillhandahållas i fritextfältet.

Mänskligt misstag: Incidenten orsakades av en persons oavsiktliga misstag, antingen som en del av betalningsförfarandet (t.ex. uppladdning av fel kommandofil för betalningar i betalningssystemet) eller på något sätt kopplat till detta (t.ex. om strömförsörjningen av en olyckshändelse bryts och betalningsoperationen avbryts). Dessa delas in i följande kategorier:

Oavsiktliga misstag, nämligen fel, utelämnanden, brist på erfarenhet och kunskap.
Avsaknad av åtgärder, t.ex. på grund av brist på kompetens, kunskap, erfarenhet, medvetenhet.
Otillräckliga resurser: t.ex. brist på mänskliga resurser, tillgång till personal.
Annat (precisera): Orsaken till incidenten är inte något av ovanstående. Ytterligare uppgifter ska tillhandahållas i fritextfältet.

Extern händelse: Orsaken är kopplad till händelser som på ett generellt plan ligger utanför organisationens kontroll. Dessa delas in i följande kategorier:

Fel från en leverantörs eller en teknisk tjänsteleverantörs sida, t.ex. elavbrott, internetavbrott, rättsliga frågor, verksamhetsfrågor, beroende av tjänster.
Force majeure t.ex. elavbrott, bränder, naturliga orsaker såsom jordbävningar, översvämningar, kraftig nederbörd, hårda vindar.
Annat (precisera): Orsaken till incidenten är inte något av ovanstående. Ytterligare uppgifter ska tillhandahållas i fritextfältet.

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

Annan relevant information om den underliggande orsaken: Ange ytterligare upplysningar om den underliggande orsaken och inkludera de preliminära slutsatserna från analysen av de underliggande orsakerna.

Huvudsakliga korrigerande åtgärder/åtgärder som vidtagits eller planeras för att förhindra att incidenten inträffar igen, om dessa är kända: Beskriv de huvudsakliga åtgärder som vidtagits eller planeras för att förhindra att incidenten inträffar igen.

C 3 – Ytterligare uppgifter

Har andra betaltjänstleverantörer informerats om incidenten? 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 inletts mot betaltjänstleverantören? Ange om betaltjänstleverantören vid den tidpunkt då slutrapporten fylls i har blivit föremål för rättsliga åtgärder (t.ex. dragits inför domstol eller förlorat sin licens) till följd av incidenten.

Bedömning av effektiviteten av utförda handlingar: Inkludera om tillgängligt en självbedömning avseende effektiviteten av de åtgärder som vidtagits under den tid som incidenten pågått, och beskriv eventuella lärdomar som dragits genom incidenthanteringen.