EBA/GL/2017/10

19/12/2017

Richtsnoeren

voor de melding van grote incidenten uit hoofde van Richtlijn (EU) 2015/2366 (PSD2)

1. Nalevings- en rapportageverplichtingen

Status van deze richtsnoeren

1. Dit document bevat richtsnoeren die zijn uitgebracht op grond van artikel 16 van Verordening (EU) nr. 1093/2010[1]. Overeenkomstig artikel 16, lid 3, van Verordening (EU) nr. 1093/2010 moeten bevoegde autoriteiten en financiële instellingen zich tot het uiterste inspannen om aan die richtsnoeren te voldoen.

2. Richtsnoeren geven weer wat in de opvatting van de EBA passende toezichtpraktijken binnen het Europees Systeem voor financieel toezicht zijn en hoe het recht van de Unie op een specifiek gebied dient te worden toegepast. Bevoegde autoriteiten als bedoeld in artikel 4, lid 2, van Verordening (EU) nr. 1093/2010 voor wie richtsnoeren gelden, dienen hieraan te voldoen door deze op passende wijze in hun praktijken te integreren (bijvoorbeeld door hun wettelijk kader of hun toezichtprocessen aan te passen), ook wanneer richtsnoeren primair tot instellingen zijn gericht.

Kennisgevingsverplichtingen

3. Overeenkomstig artikel 16, lid 3, van Verordening (EU) nr. 1093/2010 stellen bevoegde autoriteiten EBA vóór 19.02.2018 ervan in kennis of zij aan deze richtsnoeren voldoen of voornemens zijn deze op te volgen, of, indien dit niet het geval is, wat de redenen van de niet-naleving zijn. Bevoegde autoriteiten die bij het verstrijken van de termijn niet hebben gereageerd, worden geacht niet te hebben voldaan aan de richtsnoeren. Kennisgevingen worden ingediend door het formulier op de EBA-website te versturen naar compliance@eba.europa.eu onder vermelding van "EBA/GL/2017/10". Kennisgevingen worden ingediend door personen die bevoegd zijn om namens hun bevoegde autoriteiten te melden of zij aan de richtsnoeren voldoen. Elke verandering in de status van de naleving dient eveneens aan EBA te worden gemeld.

4. Kennisgevingen worden overeenkomstig artikel 16, lid 3, van de EBA-verordening op haarwebsite bekendgemaakt.

[1] Verordening (EU) nr. 1093/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Bankautoriteit), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/78/EG van de Commissie (PB L 331 van 15.12.2010, blz. 12).

2. Onderwerp, toepassingsgebied en definities

Onderwerp

5. Deze richtsnoeren vloeien voort uit de opdracht die aan EBA is gegeven in artikel 96, lid 3, van Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG (PSD2).

6. Deze richtsnoeren verschaffen met name de criteria voor de classificatie van grote operationele en veiligheidsincidenten door betalingsdienstaanbieders, evenals het formaat en de procedures die zij dienen te volgen om de bevoegde autoriteit in de lidstaat van herkomst in kennis te stellen van dergelijke incidenten, zoals bepaald in artikel 96, lid 1, van de bovengenoemde richtlijn.

7. Bovendien behandelen deze richtsnoeren de manier waarop deze bevoegde autoriteiten de relevantie van het incident beoordelen en de bijzonderheden uit de incidentmeldingen die zij, overeenkomstig artikel 96, lid 2, van de genoemde richtlijn, dienen te delen met andere binnenlandse autoriteiten.

8. Deze richtsnoeren behandelen ook het delen van de relevante bijzonderheden van de gemelde incidenten met EBA en de ECB teneinde een gemeenschappelijke, consistente aanpak te bevorderen.

Toepassingsgebied

9. Deze richtsnoeren gelden met betrekking tot de classificatie en de melding van grote operationele en veiligheidsincidenten overeenkomstig artikel 96 van Richtlijn (EU) 2015/2366.

10. Deze richtsnoeren gelden voor alle incidenten die onder de definitie vallen van ‘groot operationeel of veiligheidsincident’; hieronder vallen zowel externe als interne gebeurtenissen die door kwade wil of per ongeluk kunnen zijn ontstaan.

11. Deze richtsnoeren gelden ook wanneer het grote operationele of veiligheidsincident zijn oorsprong vindt buiten de Unie (bijv. wanneer een incident zijn oorsprong vindt in het moederbedrijf of in een buiten de Unie gevestigde dochteronderneming) en direct (een betalingsgerelateerde dienst wordt uitgevoerd door de getroffen onderneming buiten de Unie) dan wel indirect (het vermogen van de betalingsdienstaanbieder om zijn betalingsactiviteiten te blijven verrichten, wordt op de een of andere manier in gevaar gebracht als gevolg van het

incident) gevolgen heeft voor de betalingsdiensten van een in de Unie gevestigde betalingsdienstaanbieder .

Adressaten

12. De eerste reeks richtsnoeren (hoofdstuk 4) is gericht tot betalingsdienstaanbieders als gedefinieerd in artikel 4, lid 11, van Richtlijn (EU) 2015/2366 en vermeld in artikel 4, lid1, van Verordening (EU) 1093/2010.

13. De tweede en derde reeks richtsnoeren (hoofdstukken 5 en 6) zijn gericht tot bevoegde autoriteiten als gedefinieerd in artikel 4, lid 2, onder i) van Verordening (EU) nr. 1093/2010.

Definities

14. Tenzij anders aangegeven hebben de termen die in Richtlijn (EU) 2015/2366 worden gebruikt en gedefinieerd, in deze richtsnoeren dezelfde betekenis. In deze richtsnoeren gelden bovendien de volgende definities:

Operationeel of veiligheidsincident	Een op zichzelf staande gebeurtenis of een reeks met elkaar verbonden gebeurtenissen die niet is gepland door de betalingsdienstaanbieder en die een nadelig effect heeft of waarschijnlijk zal hebben op de integriteit, beschikbaarheid, vertrouwelijkheid, authenticiteit en/of continuïteit van betalingsgerelateerde diensten.
Integriteit	De eigenschap dat de juistheid en de volledigheid van activa (waaronder gegevens) wordt gewaarborgd.
Beschikbaarheid	De eigenschap van betalingsgerelateerde diensten dat ze toegankelijk zijn voor betalingsdienstgebruikers en door hen kunnen worden gebruikt.
Vertrouwelijkheid	De eigenschap dat informatie niet beschikbaar wordt gesteld voor of verstrekt aan niet-geautoriseerde personen, entiteiten of processen.
Authenticiteit	De eigenschap van een bron dat deze is wat hij beweert te zijn.
Continuïteit	De eigenschap van de voor de levering van betalingsgerelateerde diensten noodzakelijke processen, taken en activa van een organisatie dat ze volledig toegankelijk zijn en functioneren op aanvaardbare, vooraf vastgelegde niveaus.
Betalingsgerelateerde diensten	Iedere zakelijke activiteit in de zin van artikel 4, lid 3, van PSD2, en alle vereiste technische ondersteunende taken voor de correcte levering van betalingsdiensten.

3. Uitvoering

Toepassingsdatum

15. Deze richtsnoeren gelden vanaf 13 januari 2018.

4. Richtsnoeren gericht tot betalingsdienstaanbieders betreffende de melding van grote operationele of veiligheidsincidenten aan de bevoegde autoriteit in hun lidstaat van herkomst

Richtsnoer 1: Classificatie als groot incident

1.1. Betalingsdienstaanbieders classificeren operationele of veiligheidsincidenten als 'groot' wanneer deze voldoen aan

a. een of meer criteria op het niveau 'Grote impact', of

b. drie of meer criteria op het niveau 'Enige impact'

als vermeld in richtsnoer 1.4, en volgens de in deze richtsnoeren omschreven beoordeling.

1.2. Betalingsdienstaanbieders beoordelen een operationeel of veiligheidsincident aan de hand van de volgende criteria en hun onderliggende indicatoren:

i. Getroffen transacties

Betalingsdienstaanbieders bepalen de totale waarde van de getroffen transacties en het aantal getroffen betalingen als percentage van het normale aantal betalingstransacties dat is uitgevoerd met de getroffen betalingsdiensten.

ii. Getroffen betalingsdienstgebruikers

Betalingsdienstaanbieders bepalen het aantal getroffen betalingsdienstgebruikers, in absolute cijfers en als percentage van het totale aantal betalingsdienstgebruikers.

iii. Uitvaltijd dienstverlening

Betalingsdienstaanbieders bepalen de tijdsduur dat de dienst waarschijnlijk niet beschikbaar zal zijn voor de gebruiker van de betalingsdienst, of dat de betalingsopdracht in de zin van artikel 4, lid13, van PSD2 niet kan worden uitgevoerd door de betalingsdienstaanbieder.

iv. Economische gevolgen

Betalingsdienstaanbieders bepalen de financiële kosten die aan het incident zijn verbonden als totaal, en houden zowel rekening met het absolute bedrag als, waar van toepassing, met het relatieve belang van deze kosten in verhouding tot de omvang van de betalingsdienstaanbieder (d.w.z. tot het tier 1-kapitaal van de betalingsdienstaanbieder).

v. Hoog niveau van interne escalatie

Betalingsdienstaanbieders bepalen of dit incident is gemeld of waarschijnlijk zal worden gemeld aan hun hoogste leidinggevenden.

vi. Mogelijke gevolgen voor andere betalingsdienstaanbieders of relevante infrastructuren

Betalingsdienstaanbieders bepalen de gevolgen die het incident waarschijnlijk zal hebben voor het systeem, dat wil zeggen het potentieel van het incident om niet alleen gevolgen te hebben voor de aanvankelijk getroffen betalingsdienstaanbieder maar ook voor andere betalingsdienstaanbieders, financiële-marktinfrastructuren en/of kaartbetalingssystemen.

vii. Gevolgen voor de reputatie

Betalingsdienstaanbieders bepalen hoe het incident het vertrouwen van gebruikers in de betalingsdienstaanbieder zelf en meer in het algemeen in de onderliggende dienst of de markt als geheel kan ondermijnen.

1.3. Betalingsdienstaanbieders berekenen de waarde van de indicatoren aan de hand van de volgende methode:

i. Getroffen transacties

In het algemeen verstaan betalingsdienstaanbieders onder 'getroffen transacties' alle binnenlandse en grensoverschrijdende transacties die direct of indirect gevolgen ondervinden of waarschijnlijk zullen ondervinden van het incident, en in het bijzonder de transacties die niet konden worden geïnitieerd of verwerkt, de transacties waarvoor de inhoud van het betalingsbericht werd veranderd en de transacties waartoe op frauduleuze wijze opdracht is gegeven (ongeacht de vraag of het geld al dan niet is teruggevorderd).

Daarnaast beschouwen betalingsdienstaanbieders als het normale niveau van betalingstransacties het jaargemiddelde van de dagelijkse binnenlandse en grensoverschrijdende betalingstransacties die zijn uitgevoerd met dezelfde betalingsdiensten als die welke door het incident zijn getroffen, met het voorgaande jaar als de referentieperiode voor de berekeningen. Als betalingsdienstaanbieders dit cijfer als niet-representatief beschouwen (bijv. wegens seizoenseffecten), gebruiken zij in plaats daarvan een andere, representatievere maatstaf en verstrekken zij de bevoegde autoriteit de redenen voor deze aanpak in het desbetreffende veld van het formulier (zie bijlage 1).

ii. Getroffen betalingsdienstgebruikers

Betalingsdienstaanbieders verstaan onder ‘getroffen betalingsdienstgebruikers’ alle klanten (uit binnen- en buitenland, zowel consumenten als bedrijven) die een contract hebben met de getroffen betalingsdienstaanbieder dat hen toegang geeft tot de getroffen betalingsdienst, en die gevolgen van het incident hebben ondervonden of waarschijnlijk zullen ondervinden. Betalingsdienstaanbieders maken gebruik van schattingen op basis van activiteiten in het verleden om vast te stellen hoeveel betalingsdienstgebruikers tijdens de duur van het incident mogelijk de betalingsdienst hebben gebruikt.

In het geval van groepen kijkt elke betalingsdienstaanbieder alleen naar zijn eigen betalingsdienstgebruikers. Een betalingsdienstaanbieder die operationele diensten aanbiedt

aan anderen, kijkt alleen naar de gebruikers van zijn eigen betalingsdienst (indien die er zijn); de betalingsdienstaanbieders die deze operationele diensten gebruiken, beoordelen het incident met betrekking tot hun eigen betalingsdienstgebruikers.

Bovendien beschouwen betalingsdienstaanbieders als het totale aantal betalingsdienstgebruikers het totaalcijfer van betalingsdienstgebruikers in binnen- en buitenland die ten tijde van het incident contractueel aan hen zijn gebonden (of eventueel het meest recente beschikbare cijfer) en die toegang hadden tot de getroffen betalingsdienst, ongeacht hoe groot ze zijn en of zij worden beschouwd als actieve of passieve betalingsdienstgebruikers.

iii. Uitvaltijd dienstverlening

Betalingsdienstaanbieders houden rekening met de tijd gedurende welke een met de levering van betalingsdiensten samenhangende taak, proces of kanaal niet beschikbaar is of waarschijnlijk niet beschikbaar zal zijn en daarmee (i) het initiëren en/of de uitvoering van een betalingsdienst en/of (ii) de toegang tot een betaalrekening onmogelijk is. Betalingsdienstaanbieders stellen de uitvaltijd van de dienstverlening vast vanaf het moment dat de dienst uitvalt, en zij houden rekening met zowel de perioden dat zij open zijn voor de uitvoering van betalingsdiensten als de sluitings- en onderhoudsperioden, voor zover relevant en toepasselijk, mee. Als betalingsdienstaanbieders niet in staat zijn vast te stellen wanneer de uitval is begonnen, rekenen zij de uitvaltijd bij wijze van uitzondering vanaf het moment dat deze aan het licht is gekomen.

iv. Economische gevolgen

Betalingsdienstaanbieders houden rekening met zowel de kosten die direct aan het incident kunnen worden gerelateerd als de kosten die indirect met het incident samenhangen. Betalingsdienstaanbieders houden onder meer rekening met onteigend geld of onteigende activa, vervangingskosten van hardware of software, andere forensische of herstelkosten, vergoedingen als gevolg van niet-nakoming van contractuele verplichtingen, sancties, externe verplichtingen en gederfde inkomsten. Wat de indirecte kosten betreft houden betalingsdienstaanbieders alleen rekening met de indirecte kosten die al bekend zijn of waarvan het zeer waarschijnlijk is dat ze zich zullen voordoen.

v. *Hoog niveau van interne escalatie*

Betalingsdienstaanbieders houden rekening met de vraag of, als gevolg van de impact van het incident op betalingsgerelateerde diensten, de Chief Information Officer (of een vergelijkbare functie) al of niet op de hoogte is gesteld of waarschijnlijk zal worden gesteld van het incident buiten een eventuele periodieke kennisgevingsprocedure en op een continue basis tijdens de gehele duur van het incident. Bovendien houden betalingsdienstaanbieders rekening met de vraag of als gevolg van de impact van het incident op betalingsgerelateerde diensten een crisismodus is geïnitieerd of waarschijnlijk zal worden geïnitieerd.

vi. *Mogelijke gevolgen voor andere betalingsdienstaanbieders of relevante infrastructuren*

Betalingsdienstaanbieders beoordelen de impact van het incident op de financiële markt, waarbij onder financiële markt wordt verstaan de financiële-marktinfrastructuren en/of kaartbetalingschemas die hen en andere betalingsdienstaanbieders ondersteunen. Met name beoordelen betalingsdienstaanbieders of het incident zich heeft herhaald of zich waarschijnlijk zal herhalen bij andere betalingsdienstaanbieders, of het de probleemloze werking van financiële-marktinfrastructuren heeft verstoord of waarschijnlijk zal verstoren en of het de goede werking van het financiële systeem als geheel in gevaar heeft gebracht of waarschijnlijk in gevaar zal brengen. Betalingsdienstaanbieders houden rekening met diverse aspecten, zoals de vraag of het om een eigen of algemeen verkrijgbare component/software gaat, of het getroffen netwerk intern of extern is en of de betalingsdienstaanbieder is gestopt of waarschijnlijk zal stoppen met het voldoen aan zijn verplichtingen in de financiële marktinfrastructuren waarvan hij lid is.

vii. *Gevolgen voor de reputatie*

Betalingsdienstaanbieders houden rekening met de mate van zichtbaarheid die het incident, voor zover hun bekend is, heeft gekregen of waarschijnlijk zal krijgen in de markt. Met name houden betalingsdienstaanbieders rekening met de waarschijnlijkheid dat het incident schade zal toebrengen aan de maatschappij, als een goede indicator van het potentieel van het incident om hun reputatie aan te tasten. Betalingsdienstaanbieders houden rekening met de vraag of (i) het incident gevolgen heeft gehad voor een zichtbaar proces en daardoor waarschijnlijk aandacht zal krijgen in de media of die aandacht al heeft gekregen (waarbij niet alleen wordt gekeken naar traditionele media zoals kranten, maar ook naar blogs, sociale netwerken, enz.), (ii) wettelijke verplichtingen niet zijn nagekomen of waarschijnlijk niet zullen worden nagekomen, (iii) sancties zijn genegeerd of waarschijnlijk zullen worden genegeerd, of (iv) hetzelfde incident zich eerder heeft voorgedaan.

1.4. Betalingsdienstaanbieders beoordelen een incident door voor elk criterium vast te stellen of de relevante drempels in tabel 1 zijn bereikt of waarschijnlijk zullen worden bereikt voordat het incident is opgelost.

Tabel 1: Drempels

Criterium	Enige impact	Grote impact
Getroffen transacties	> 10% van het normale aantal transacties van de betalingsdienstaanbieder **en** > 100 000 EUR	> 25% van het normale aantal transacties van de betalingsdienstaanbieder **of** > 5 miljoen EUR
Getroffen betalingsdienstgebruikers	> 5 000 **en** > 10% van de gebruikers van de betalingsdienstaanbieder	> 50 000 **of** > 25% van de gebruikers van de betalingsdienstaanbieder
Uitvaltijd dienstverlening	> 2 uur	Niet van toepassing
Economische gevolgen	Niet van toepassing	> Max. (0,1% tier 1-kapitaal,* 200 000 EUR) **of** > 5 miljoen EUR
Hoog niveau van interne escalatie	Ja	Ja, en er zal waarschijnlijk een crisismodus (of vergelijkbare modus) worden geïnitieerd
Mogelijke gevolgen voor andere betalingsdienstaanbieders of relevante infrastructuren	Ja	Niet van toepassing
Gevolgen voor de reputatie	Ja	Niet van toepassing

*Tier 1-kapitaal als gedefinieerd in artikel 25 van Verordening (EU) nr. 575/2013 van het Europees Parlement en de Raad van 26 juni 2013 betreffende prudentiële vereisten voor kredietinstellingen en beleggingsondernemingen en tot wijziging van Verordening (EU) nr. 648/2012.

1.5. Betalingsdienstaanbieders maken gebruik van schattingen als zij niet beschikken over werkelijke gegevens ter ondersteuning van hun beoordelingen van de vraag of een bepaalde drempel is bereikt of waarschijnlijk zal worden bereikt voordat het incident is opgelost (dit kan zich bijvoorbeeld voordoen tijdens de eerste onderzoeksfase).

1.6. Betalingsdienstaanbieders voeren deze beoordeling op continue basis uit tijdens de duur van het incident teneinde een mogelijke statusverandering in opwaartse (van niet groot naar groot) of neerwaartse (van groot naar niet groot) richting te identificeren.

Richtsnoer 2: Meldingsproces

2.1. Betalingsdienstaanbieders verzamelen alle relevante informatie, stellen een incidentmelding op met behulp van het in bijlage 1 verstrekte formulier en dienen dit in bij de bevoegde autoriteit in de lidstaat van herkomst. Betalingsdienstaanbieders vullen het formulier in volgens de in bijlage 1 gegeven instructies.

2.2. Betalingsdienstaanbieders gebruiken hetzelfde formulier om de bevoegde autoriteit tijdens de volledige duur van het incident te informeren (d.w.z. voor initiële, tussentijdse en eindmeldingen, zoals omschreven in de paragrafen 2.7 tot en met 2.21). Betalingsdienstaanbieders vullen het formulier stapsgewijs en naar beste vermogen in naarmate meer informatie beschikbaar komt tijdens hun interne onderzoeken.

2.3. Betalingsdienstaanbieders verstrekken de bevoegde autoriteit in hun lidstaat van herkomst, wanneer van toepassing, ook een kopie van de informatie die zij hebben verstrekt (of zullen verstrekken) aan hun gebruikers overeenkomstig artikel 96, lid 1, tweede alinea, van PSD2, zodra deze beschikbaar is.

2.4. Betalingsdienstaanbieders verstrekken de bevoegde autoriteit in de lidstaat van herkomst aanvullende informatie, indien deze beschikbaar is en relevant wordt geacht voor de bevoegde autoriteit, door aanvullende documenten als een of meer bijlagen aan het gestandaardiseerde formulier toe te voegen.

2.5. Betalingsdienstaanbieders voldoen aan elk verzoek van de bevoegde autoriteit in de lidstaat van herkomst tot het verstrekken van aanvullende informatie of verduidelijkingen van reeds ingediende documentatie.

2.6. Betalingsdienstaanbieders waarborgen te allen tijde de vertrouwelijkheid en de integriteit van de informatie die zij uitwisselen met de bevoegde autoriteit in hun lidstaat van herkomst en authenticeren zich naar behoren tegenover de bevoegde autoriteit in hun lidstaat van herkomst.

Initiële melding

2.7. Betalingsdienstaanbieders dienen een initiële melding in bij de bevoegde autoriteit in hun lidstaat van herkomst wanneer een groot operationeel of veiligheidsincident wordt ontdekt.

2.8. Betalingsdienstaanbieders zenden de initiële melding naar de bevoegde autoriteit binnen 4 uur na het moment waarop het grote operationele of veiligheidsincident wordt ontdekt of, als bekend is dat de meldingskanalen van de bevoegde autoriteit op dat tijdstip niet beschikbaar of niet operationeel zijn, zodra deze weer beschikbaar/operationeel zijn.

2.9. Betalingsdienstaanbieders dienen ook een initiële melding in bij de bevoegde autoriteit in de lidstaat van herkomst wanneer een incident dat eerder niet groot was, een groot incident wordt. In dit speciale geval sturen betalingsdienstaanbieders de initiële melding onmiddellijk nadat de veranderde status is vastgesteld, naar de bevoegde autoriteit, of, als bekend is dat de meldingskanalen van de bevoegde autoriteit op dat tijdstip niet beschikbaar of niet operationeel zijn, zodra deze weer beschikbaar/operationeel zijn.

2.10. Betalingsdienstaanbieders nemen kerngegevens (d.w.z. rubriek A van het formulier) op in hun initiële melding; zij vermelden enkele basiskenmerken van het incident en de te verwachte gevolgen ervan op basis van de informatie die onmiddellijk beschikbaar is nadat het incident is ontdekt of de classificatie ervan is gewijzigd. Betalingsdienstaanbieders maken gebruik van schattingen wanneer er geen werkelijke gegevens beschikbaar zijn. Betalingsdienstaanbieders nemen in hun initiële melding ook de datum voor de volgende update op; deze dient zo spoedig mogelijk te zijn en mag in geen geval later zijn dan 3 werkdagen na de initiële melding.

Tussentijdse melding

2.11. Betalingsdienstaanbieders dienen telkens wanneer zij menen dat er een belangrijke statuswijziging is, tussentijdse meldingen in, maar in ieder geval op het tijdstip van de volgende update dat vermeld is in de voorgaande melding (de initiële melding of de voorgaande tussentijdse melding).

2.12. Betalingsdienstaanbieders dienen bij de bevoegde autoriteit een eerste tussentijdse melding in met een gedetailleerdere beschrijving van het incident en de gevolgen daarvan (rubriek B van het formulier). Bovendien stellen betalingsdienstaanbieders aanvullende tussentijdse meldingen op door de informatie die al verstrekt is in de rubrieken A en B van het formulier bij te werken wanneer zij kennis krijgen van nieuwe relevante informatie of significante veranderingen sinds de voorgaande melding (bijv. of het incident ernstiger of minder ernstig is geworden, er nieuwe oorzaken zijn vastgesteld of acties zijn ondernomen om het probleem op te lossen). Betalingsdienstaanbieders stellen in ieder geval een tussentijdse melding op wanneer de bevoegde autoriteit in de lidstaat van herkomst daarom verzoekt.

2.13. Net als bij initiële meldingen maken betalingsdienstaanbieders gebruik van schattingen wanneer werkelijke gegevens niet beschikbaar zijn.

2.14. Bovendien vermelden betalingsdienstaanbieders in elke melding de datum voor de volgende update; deze dient zo spoedig mogelijk te zijn en mag in geen geval later zijn dan 3 werkdagen na de melding. Indien de betalingsdienstaanbieder niet in staat is een volgende update in te dienen op de geschatte datum, neemt hij contact op met de bevoegde autoriteit om de redenen voor de vertraging toe te lichten, stelt hij een nieuwe, aannemelijke uiterste datum voor indiening voor (niet later dan na 3 werkdagen) en stuurt hij een nieuwe tussentijdse melding waarin uitsluitend de informatie over de geschatte datum van de volgende update wordt bijgewerkt.

2.15. Wanneer de reguliere activiteiten zijn hersteld en de situatie weer normaal is, sturen betalingsdienstaanbieders de laatste tussentijdse melding, waarin ze de bevoegde autoriteit hiervan op de hoogte stellen. Betalingsdienstaanbieders beschouwen de situatie als weer normaal wanneer de activiteiten in termen van verwerkingstijden, capaciteit, veiligheidsvereisten, etc., weer plaatsvinden op hetzelfde dienstverleningsniveau en/of onder dezelfde omstandigheden als gedefinieerd door de betalingsdienstaanbieder of als extern vastgelegd in een Service Level Agreement (SLA), en als er geen noodmaatregelen meer van kracht zijn.

2.16. Indien de situatie weer normaal is binnen 4 uur nadat het incident is ontdekt, streven betalingsdienstaanbieders ernaar de initiële melding en de laatste tussentijdse melding gelijktijdig in te dienen (d.w.z. dat zij de rubrieken A en B van het formulier invullen) binnen de termijn van 4 uur.

Eindmelding

2.17. Betalingsdienstaanbieders sturen een eindmelding wanneer de analyse van de onderliggende oorzaak is uitgevoerd (ongeacht de vraag of er al risicobeperkende maatregelen zijn getroffen of de daadwerkelijke oorzaak is vastgesteld) en er feitelijke cijfers beschikbaar zijn ter vervanging van eventuele schattingen.

2.18. Betalingsdienstaanbieders sturen de eindmelding binnen 2 weken nadat de situatie weer normaal is geworden naar de bevoegde autoriteit. Betalingsdienstaanbieders die verlenging van deze uiterste termijn nodig hebben (bijv. als er nog geen werkelijke cijfers over de impact beschikbaar zijn), nemen contact op met de bevoegde autoriteit voordat de termijn is verstreken en verstrekken een afdoende verklaring voor de vertraging, evenals een nieuwe geschatte datum voor de eindmelding.

2.19. Indien betalingsdienstaanbieders in staat zijn alle voor de eindmelding vereiste informatie (d.w.z. rubriek C van het formulier) te verstrekken binnen de termijn van 4 uur sinds het incident is ontdekt, streven zij ernaar in hun initiële melding alle informatie voor de initiële, de laatste tussentijdse en de eindmelding in te dienen.

2.20. Betalingsdienstaanbieders streven ernaar in hun eindmelding volledige informatie op te nemen, d.w.z. (i) feitelijke cijfers over de impact in plaats van schattingen (evenals eventuele andere vereiste aanpassingen in de rubrieken A en B van het formulier) en (ii) rubriek C van het formulier, met daarin de onderliggende oorzaak, indien al bekend, en een samenvatting van maatregelen die zijn genomen of gepland om het probleem te verhelpen en te voorkomen dat het zich in de toekomst opnieuw voordoet.

2.21. Betalingsdienstaanbieders sturen ook een eindmelding wanneer zij, als resultaat van de continue beoordeling van het incident, vaststellen dat een reeds gemeld incident niet langer voldoet aan de criteria voor een groot incident en niet wordt verwacht dat het daaraan weer zal voldoen voordat het is opgelost. In dit geval sturen betalingsdienstaanbieders de eindmelding zodra deze omstandigheid wordt vastgesteld en uiterlijk op de geschatte datum voor de volgende melding. In deze specifieke situatie vullen betalingsdienstaanbieders niet rubriek C van het formulier in, maar vinken zij het vakje ‘Incident geherclassificeerd als niet groot’ aan en leggen zij uit waarom het incident naar een lager niveau is teruggebracht.

Richtsnoer 3: Gedelegeerde en geconsolideerde meldingen

3.1. Waar dit is toegestaan door de bevoegde autoriteit, stellen betalingsdienstaanbieders die meldingsverplichtingen uit hoofde van PSD2 willen delegeren aan een derde partij, de bevoegde autoriteit in de lidstaat van herkomst hiervan op de hoogte en zorgen zij ervoor dat aan de volgende voorwaarden wordt voldaan:

a. In het formele contract of, indien van toepassing, de bestaande interne regelingen binnen een groep, die de grondslag vormen voor de gedelegeerde meldingen tussen de derde partij en de betalingsdienstaanbieder worden de aan alle partijen toegewezen verantwoordelijkheden ondubbelzinnig vastgelegd. Met name wordt duidelijk bepaald dat, ongeacht de eventuele delegering van meldingsverplichtingen de getroffen betalingsdienstaanbieder volledig verantwoordelijk en aansprakelijk blijft voor het voldoen aan de vereisten die zijn vastgelegd in artikel 96 van PSD2 en voor de inhoud van de informatie die wordt verstrekt aan de bevoegde autoriteit van de lidstaat van herkomst.

b. De delegering voldoet aan de vereisten voor de uitbesteding van belangrijke operationele taken als uiteengezet in

   i. artikel 19, lid 6, van PSD2 met betrekking tot betalingsinstellingen en instellingen voor elektronisch geld, mutatis mutandis toepasselijk overeenkomstig artikel 3 van Richtlijn 2009/110/EG; of

   ii. de uitbestedingsrichtsnoeren van het CEBT met betrekking tot kredietinstellingen.

c. De informatie wordt vooraf ingediend bij de bevoegde autoriteit in de lidstaat van herkomst en in ieder geval overeenkomstig de uiterste termijnen en procedures die zijn vastgesteld door de bevoegde autoriteit, waar van toepassing.

d. De vertrouwelijkheid van gevoelige gegevens en de kwaliteit, consistentie, integriteit en betrouwbaarheid van de aan de bevoegde autoriteit te verstrekken informatie is naar behoren gewaarborgd.

3.2. Betalingsdienstaanbieders die de aangewezen derde partij ertoe in staat willen stellen op een geconsolideerde wijze te voldoen aan de meldingsverplichtingen (bijv. door één melding in te dienen die betrekking heeft op verscheidene betalingsdienstaanbieders die getroffen zijn door hetzelfde grote operationele of veiligheidsincident), stellen de bevoegde autoriteit in de lidstaat van herkomst hiervan in kennis, vermelden daarbij de contactinformatie onder 'Getroffen betalingsdienstaanbieder' in het formulier en zorgen ervoor dat aan de volgende voorwaarden wordt voldaan:

a. Deze bepaling wordt opgenomen in het contract dat de grondslag vormt voor de gedelegeerde melding.

b. Als voorwaarde voor de geconsolideerde melding geldt dat het incident wordt veroorzaakt door een verstoring van de diensten die door de derde partij worden geleverd.

c. De geconsolideerde melding wordt beperkt tot betalingsdienstaanbieders die in dezelfde lidstaat zijn gevestigd.

d. Er wordt gewaarborgd dat de derde partij het belang van het incident voor elke getroffen betalingsdienstaanbieder beoordeelt en in de geconsolideerde melding alleen die betalingsdienstaanbieders opneemt waarvoor het incident als groot wordt geclassificeerd. Bovendien wordt gewaarborgd dat bij twijfel een betalingsdienstaanbieder in de geconsolideerde melding blijft opgenomen zolang er geen bewijs is dat hij hierin niet hoeft te worden opgenomen.

e. Er wordt gewaarborgd dat, wanneer er velden van het formulier zijn waar een gemeenschappelijk antwoord niet mogelijk is (bijv. rubriek B 2, B 4 of C 3), de derde partij ofwel (i) deze apart invult voor elke getroffen betalingsdienstaanbieder, waarbij hij specificeert op welke betalingsdienstaanbieder de informatie betrekking heeft, ofwel (ii) bandbreedtes gebruikt in de velden waar dat een mogelijkheid is, met de laagste en de hoogste waarde die is vastgesteld of geschat voor de verschillende betalingsdienstaanbieders.

f. Betalingsdienstaanbieders waarborgen dat de derde partij hen te allen tijde op de hoogte houdt van alle relevante informatie met betrekking tot het incident en alle interacties die de derde partij mogelijk heeft met de bevoegde autoriteit en de inhoud daarvan, maar slechts voor zover dit geen schending inhoudt van de vertrouwelijkheid van de informatie met betrekking tot andere betalingsdienstaanbieders.

3.3. Betalingsdienstaanbieders delegeren hun meldingsverplichtingen niet voordat zij de bevoegde autoriteit in de lidstaat van herkomst hiervan op de hoogte hebben gesteld of nadat hun is meegedeeld dat de uitbestedingsovereenkomst niet voldoet aan de vereisten die zijn genoemd in richtsnoer 3.1, onder b).

3.4. Betalingsdienstaanbieders die de delegering van hun meldingsverplichtingen willen intrekken, stellen de bevoegde autoriteit in de lidstaat van herkomst van dit besluit op de hoogte met inachtneming van de uiterste termijnen en procedures van die bevoegde autoriteit. Betalingsdienstaanbieders stellen de bevoegde autoriteit in de lidstaat van herkomst ook op de hoogte van iedere belangrijke ontwikkeling met betrekking tot de aangewezen derde partij die van invloed is op het vermogen van die derde partij om aan de meldingsverplichtingen te voldoen.

3.5. Wanneer de aangewezen derde partij verzuimt de bevoegde autoriteit in de lidstaat van herkomst te informeren over een groot operationeel of veiligheidsincident overeenkomstig artikel 96 van PSD2 en deze richtsnoeren, vervullen betalingsdienstaanbieders hun meldingsverplichtingen zonder externe hulp in te schakelen. Bovendien zorgen betalingsdienstaanbieders ervoor dat een incident niet twee keer wordt gemeld, afzonderlijk door de betalingsdienstaanbieder en nog eens door de derde partij.

Richtsnoer 4: Operationeel en veiligheidsbeleid

4.1. Betalingsdienstaanbieders zorgen ervoor dat alle verantwoordelijkheden voor de melding van incidenten uit hoofde van PSD2, evenals de ten uitvoer gelegde processen om te voldoen aan de in deze richtsnoeren gedefinieerde vereisten, duidelijk zijn vastgelegd in hun algemene operationele en veiligheidsbeleid.

5. Richtsnoeren gericht tot bevoegde autoriteiten betreffende de criteria voor de beoordeling van de relevantie van het incident en de bijzonderheden uit de incidentmeldingen die zij dienen te delen met andere binnenlandse autoriteiten

Richtsnoer 5: Beoordeling van de relevantie van het incident

5.1. Bevoegde autoriteiten in de lidstaat van herkomst beoordelen de relevantie van een groot operationeel of veiligheidsincident voor andere binnenlandse autoriteiten op basis van hun eigen deskundige mening en aan de hand van de volgende criteria als belangrijkste indicatoren van het belang van het incident in kwestie:

a. De oorzaken van het incident vallen onder de wettelijke bevoegdheid van de andere binnenlandse autoriteit (d.w.z. haar bevoegdheidsgebied).
b. De gevolgen van het incident zijn van invloed op de doelstellingen van een andere binnenlandse autoriteit (bijv. het waarborgen van financiële stabiliteit).
c. Het incident treft betalingsdienstgebruikers op grote schaal of kan dit gaan doen.
d. Het incident krijgt waarschijnlijk brede aandacht in de media of heeft die al gehad.

5.2. Bevoegde autoriteiten in de lidstaat van herkomst voeren deze beoordeling op continue basis uit tijdens de duur van het incident, om eventuele veranderingen vast te stellen die een incident dat eerder niet als relevant werd beschouwd, relevant kunnen maken.

Richtsnoer 6: Te delen informatie

6.1. Onverminderd eventuele andere wettelijke vereisten tot het delen van informatie over incidenten met andere binnenlandse autoriteiten, verstrekken bevoegde autoriteiten informatie over grote operationele of veiligheidsincidenten aan de binnenlandse autoriteiten die zijn vastgesteld na de toepassing van richtsnoer 5.1 (‘andere relevante binnenlandse autoriteiten’), in ieder geval op het moment dat zij de initiële melding (of de melding die aanleiding was voor het delen van informatie) ontvangen en wanneer zij ervan op de hoogte worden gesteld dat de situatie weer normaal is (de laatste tussentijdse melding).

6.2. Bevoegde autoriteiten verstrekken andere relevante binnenlandse autoriteiten de informatie die nodig is om een duidelijk beeld te krijgen van wat er is gebeurd en wat de

mogelijke gevolgen zijn. Daartoe verstrekken zij ten minste de informatie die de betalingsdienstaanbieder heeft gegeven in de volgende velden van het formulier (ofwel in de initiële melding, ofwel in de tussentijdse melding):

- datum en tijdstip van de ontdekking van het incident;
- datum en tijdstip van het begin van het incident;
- datum en tijdstip waarop het incident is hersteld of naar verwachting zal zijn hersteld;
- korte beschrijving van het incident (met inbegrip van niet-gevoelige delen van de gedetailleerde beschrijving);
- korte beschrijving van maatregelen die zijn genomen of gepland om te herstellen van het incident;
- beschrijving van hoe het incident andere betalingsdienstaanbieders en/of infrastructuren zou kunnen treffen;
- beschrijving van de media-aandacht (indien aanwezig);
- oorzaak van het incident.

6.3. Bevoegde autoriteiten zorgen waar nodig voor een adequate anonimisering en laten informatie achterwege die mogelijk vertrouwelijk is of waarop beperkingen op grond van intellectuele-eigendomsrechten rusten, voordat zij informatie over incidenten delen met andere relevante binnenlandse autoriteiten. Bevoegde autoriteiten verstrekken echter wel de naam en het adres van de meldende betalingsdienstaanbieder aan de andere relevante binnenlandse autoriteiten wanneer deze binnenlandse autoriteiten kunnen garanderen dat de informatie vertrouwelijk zal worden behandeld.

6.4. Bevoegde autoriteiten waarborgen te allen tijde de vertrouwelijkheid en de integriteit van de informatie die zij opslaan en delen met andere relevante binnenlandse autoriteiten en authenticeren zich op de juiste manier tegenover de andere relevante binnenlandse autoriteiten. Met name behandelen bevoegde autoriteiten uit hoofde van deze richtsnoeren alle ontvangen informatie overeenkomstig de bepalingen inzake beroepsgeheim van PSD2, onverminderd het toepasselijke recht van de Unie en nationale vereisten.

6. Richtsnoeren gericht tot bevoegde autoriteiten betreffende de criteria voor de beoordeling van de relevante bijzonderheden van de incidentmeldingen die zij met EBA en de ECB dienen te delen en betreffende het formaat en de procedures voor de communicatie hiervan

Richtsnoer 7: Te delen informatie

7.1. Bevoegde autoriteiten verstrekken EBA en de ECB altijd alle meldingen die zij ontvangen van (of namens) betalingsdienstaanbieders die zijn getroffen door een groot operationeel of veiligheidsincident (initiële, tussentijdse en eindmeldingen).

Richtsnoer 8: Communicatie

8.1. Bevoegde autoriteiten waarborgen te allen tijde de vertrouwelijkheid en de integriteit van de informatie die zij opslaan en delen met EBA en de ECB en authenticeren zich naar behoren tegenover EBA en de ECB. Met name behandelen bevoegde autoriteiten alle uit hoofde van deze richtsnoeren ontvangen informatie overeenkomstig de bepalingen inzake beroepsgeheim van PSD2, onverminderd het toepasselijke recht van de Unie en nationale vereisten.

8.2. Bevoegde autoriteiten zorgen voor passende communicatiemiddelen om vertragingen in de doorgifte van informatie over incidenten aan EBA/ECB te voorkomen en de risico's van operationele verstoringen zo klein mogelijk te houden.

Bijlage 1 – Formulieren voor meldingen door betalingsdienstaanbieders

CLASSIFICATION: RESTRICTED

Major Incident Report

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

Report date: DD/MM/YYYY — Time: HH:MM

Incident identification number, if applicable (for interim and final reports):

A - Initial report

A 1 - GENERAL DETAILS

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

A 2 - INCIDENT DETECTION and INITIAL CLASSIFICATION

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

B - Intermediate report

B 1 - GENERAL DETAILS

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

B 2 - INCIDENT CLASSIFICATION & INFORMATION ON THE INCIDENT

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

B 3 - INCIDENT DESCRIPTION

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

B 4 - INCIDENT IMPACT

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

B 5 - INCIDENT MITIGATION

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

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

Notes:

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

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

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

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

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

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

INSTRUCTIES VOOR HET INVULLEN VAN DE FORMULIEREN

Betalingsdienstaanbieders vullen de relevante rubriek van het formulier in afhankelijk van de meldingsfase waarin zij zich bevinden: rubriek A voor de initiële melding, rubriek B voor tussentijdse meldingen en rubriek C voor de eindmelding. Alle velden zijn verplicht tenzij duidelijk anders is aangegeven.

Kop

Initiële melding: dit is de eerste melding die de betalingsdienstaanbieder indient bij de bevoegde autoriteit in de lidstaat van herkomst.

Tussentijdse melding: dit is een update op een eerdere (initiële of tussentijdse) melding over hetzelfde incident.

Laatste tussentijdse melding: hiermee wordt de bevoegde autoriteit in de lidstaat van herkomst ervan op de hoogte gesteld dat de reguliere activiteiten zijn hersteld en dat de situatie weer normaal is, zodat er geen tussentijdse meldingen meer zullen worden ingediend.

Eindmelding: dit is de laatste melding die de betalingsdienstaanbieder over het incident zal sturen, omdat (i) er al een analyse van de onderliggende oorzaak is verricht en schattingen kunnen worden vervangen door echte cijfers, of (ii) het incident niet langer als groot wordt beschouwd.

Incident geherclassificeerd als niet groot: het incident voldoet niet langer aan de criteria om als groot te worden beschouwd en zal daar naar verwachting ook niet meer aan gaan voldoen voordat het is opgelost. Betalingsdienstaanbieders leggen uit wat de redenen zijn voor deze lagere herclassificering.

Datum en tijdstip melding: de exacte datum en het exacte tijdstip van de indiening van de melding aan de bevoegde autoriteit.

Identificatienummer incident, indien toepasselijk (voor tussentijdse meldingen en eindmelding): het referentienummer dat op het moment van de initiële melding door de bevoegde autoriteit is verstrekt als unieke identificatie van het incident, indien van toepassing (als de bevoegde autoriteit een dergelijke referentie heeft verstrekt).

A – Initiële melding

A 1 – Algemene informatie

Soort melding:

Individueel: De melding heeft betrekking op één betalingsdienstaanbieder.

Geconsolideerd: de melding heeft betrekking op verscheidene betalingsdienstaanbieders die gebruikmaken van de mogelijkheid van geconsolideerde meldingen. De velden onder 'Getroffen betalingsdienstaanbieder' blijven leeg (met uitzondering van het veld 'Door het incident getroffen land(en)') en er wordt een lijst van de in de melding opgenomen betalingsdienstaanbieders verstrekt door de desbetreffende tabel in te vullen (Geconsolideerde melding – Lijst betalingsdienstaanbieders).

Getroffen betalingsdienstaanbieder: betreft de betalingsdienstaanbieder die het incident ondervindt.

Naam betalingsdienstaanbieder: volledige naam van de betalingsdienstaanbieder die onderworpen is aan de meldingsprocedure, zoals deze luidt in het toepasselijke officiële nationale register van betalingsdienstaanbieders.

Uniek identificatienummer betalingsdienstaanbieder, indien relevant: het relevante unieke identificatienummer dat in elke lidstaat wordt gebruikt om de betalingsdienstaanbieder te identificeren; dit moet door de betalingsdienstaanbieder worden verstrekt als het veld 'Autorisatienummer betalingsdienstaanbieder' niet is ingevuld.

Autorisatienummer betalingsdienstaanbieder: autorisatienummer van de lidstaat van herkomst.

Hoofd van groep: geef in het geval van groepen entiteiten als gedefinieerd in artikel 4, lid 40, van Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG (PSD2), de naam van de hoofdentiteit op.

Land van herkomst: lidstaat waar de statutaire zetel van de betalingsdienstaanbieder zich bevindt, of, als de betalingsdienstaanbieder onder zijn nationale recht geen statutaire zetel heeft, de lidstaat waar zijn hoofdkantoor is gevestigd.

Door het incident getroffen land(en): land of landen waar het incident gevolgen heeft gehad (bijv. als verscheidene bijkantoren van een betalingsdienstaanbieder die in verschillende landen zijn gevestigd, zijn getroffen). Dit kan hetzelfde land zijn als de lidstaat van herkomst, of een ander land.

Eerste contactpersoon: voor- en achternaam van de persoon die verantwoordelijk is voor het melden van het incident of, als een derde partij de melding doet namens de getroffen betalingsdienstaanbieder, voor- en achternaam van de persoon die bij de getroffen betalingsdienstaanbieder verantwoordelijk is voor de afdeling incidentbeheer/risicobeheer of een soortgelijk aandachtsgebied.

E-mail: e-mailadres waaraan indien nodig verzoeken om nadere toelichting kunnen worden gericht. Dit kan een persoonlijk of een bedrijfsmailadres zijn.

Telefoon: het telefoonnummer dat moet worden gebeld wanneer er eventuele verzoeken om verdere verduidelijking zijn. Dit kan een persoonlijk of een bedrijfstelefoonnummer zijn.

Tweede contactpersoon: voor- en achternaam van een alternatieve persoon met wie de bevoegde autoriteit contact op kan nemen bij vragen over een incident, wanneer de eerste contactpersoon niet beschikbaar is. Als een derde partij een melding doet namens de getroffen betalingsdienstaanbieder, de voor- en achternaam van een alternatieve persoon van de afdeling incidentbeheer/risicobeheer of soortgelijk aandachtsgebied bij de getroffen betalingsdienstaanbieder.

E-mail: e-mailadres van de alternatieve contactpersoon waaraan indien nodig verzoeken om nadere toelichting kunnen worden gericht. Dit kan een persoonlijk of een bedrijfsmailadres zijn.

Telefoon: het telefoonnummer van de alternatieve contactpersoon waarnaar moet worden gebeld wanneer er eventuele verzoeken om verdere verduidelijking zijn. Dit kan een persoonlijk of een bedrijfstelefoonnummer zijn.

Meldende entiteit: dit gedeelte dient te worden ingevuld als een derde partij de meldingsverplichtingen namens de getroffen betalingsdienstaanbieder vervult.

Naam van de meldende entiteit: volledige naam van de entiteit die het incident meldt, zoals deze luidt in het toepasselijke officiële nationale bedrijvenregister.

Uniek identificatienummer, indien relevant: het relevante unieke identificatienummer dat wordt gebruikt in het land waar de derde partij is gevestigd om de entiteit die het incident meldt, te identificeren; dit dient te worden verstrekt door de meldende entiteit als het veld ‘Autorisatienummer’ niet is ingevuld.

Autorisatienummer, indien van toepassing: het autorisatienummer van de derde partij in het land waar deze is gevestigd, indien van toepassing.

Eerste contactpersoon: voor- en achternaam van de persoon die verantwoordelijk is voor het melden van het incident.

E-mail: e-mailadres waaraan indien nodig verzoeken om nadere toelichting kunnen worden gericht. Dit kan een persoonlijk of een bedrijfsmailadres zijn.
Telefoon: het telefoonnummer dat moet worden gebeld wanneer er eventuele verzoeken om verdere verduidelijking zijn. Dit kan een persoonlijk of een bedrijfstelefoonnummer zijn.
Tweede contactpersoon: voor- en achternaam van een alternatieve persoon bij de entiteit die het incident meldt, met wie de bevoegde autoriteit contact op kan nemen bij vragen over een incident, wanneer de eerste contactpersoon niet beschikbaar is.
E-mail: e-mailadres van de alternatieve contactpersoon waaraan indien nodig verzoeken om nadere toelichting kunnen worden gericht. Dit kan een persoonlijk of een bedrijfsmailadres zijn.
Telefoon: het telefoonnummer van de alternatieve contactpersoon dat moet worden gebeld wanneer er eventuele verzoeken om verdere verduidelijking zijn. Dit kan een persoonlijk of een bedrijfstelefoonnummer zijn.

A 2 – Ontdekking incident en eerste classificatie

Datum en tijdstip van de ontdekking van het incident: de datum en het tijdstip waarop het incident voor het eerst is vastgesteld.
Het incident is ontdekt door: geef aan of het incident is ontdekt door een betalingsdienstgebruiker, een andere partij binnen de betalingsdienstaanbieder (bijv. interne auditfunctie) of een externe partij (bijv. externe dienstverlener). Geef een toelichting in het daartoe bestemde veld als het geen van de bovengenoemden was.
Korte, algemene beschrijving van het incident: licht kort de belangrijkste punten van het incident toe, met vermelding van mogelijke oorzaken, onmiddellijke gevolgen, enz.
Wanneer is het verwachte moment van de volgende update? vermeld de geschatte datum en tijd voor de indiening van de volgende update (tussentijdse of eindmelding).

B – Tussentijdse melding

B 1 – Algemene informatie

Gedetailleerdere beschrijving van het incident: geef een beschrijving van de belangrijkste kenmerken van het incident, met daarin ten minste de punten die in de vragenlijst aan de orde komen (met welk specifiek probleem de betalingsdienstaanbieder wordt geconfronteerd, hoe het incident is begonnen en zich heeft ontwikkeld, of er mogelijk een verband is met een eerder incident, wat de gevolgen zijn, met name voor betalingsdienstgebruikers, enz.).
Datum en tijdstip van het begin van het incident: de datum en het tijdstip waarop het incident is begonnen, indien bekend.
Status incident:

Diagnose: de kenmerken van het incident zijn zojuist vastgesteld.
Reparatie: de aangevallen componenten worden opnieuw geconfigureerd.
Herstel: de verstoorde componenten worden teruggebracht naar de laatste toestand waarin ze kunnen worden teruggebracht.
Hervatting: de betalingsgerelateerde dienst wordt weer geleverd.

Datum en tijdstip waarop het incident is hersteld of naar verwachting zal zijn hersteld: geef de datum en het tijdstip aan waarop het incident onder controle was en de situatie weer normaal was, of wanneer dit naar verwachting het geval zal zijn.

B 2 – Classificatie incident/Informatie over het incident

Totale impact: geef aan welke aspecten gevolgen hebben ondervonden van het incident. Er kunnen meerdere antwoorden worden aangevinkt.

Integriteit: de eigenschap dat de juistheid en de volledigheid van activa (met inbegrip van gegevens) wordt gewaarborgd.

Beschikbaarheid: de eigenschap van betalingsgerelateerde diensten dat ze toegankelijk zijn voor betalingsdienstgebruikers en door hen kunnen worden gebruikt.

Vertrouwelijkheid: de eigenschap dat informatie niet beschikbaar wordt gesteld voor of verstrekt aan niet-geautoriseerde personen, entiteiten of processen.

Authenticiteit: de eigenschap van een bron dat deze is wat hij beweert te zijn.

Continuïteit: de eigenschap van de processen, taken en activa van een organisatie die nodig zijn voor de levering van betalingsgerelateerde diensten dat ze volledig toegankelijk zijn en functioneren op aanvaardbare, vooraf vastgelegde niveaus.

Getroffen transacties: Betalingsdienstaanbieders geven aan welke drempels het incident heeft bereikt of waarschijnlijk zal bereiken, indien van toepassing, evenals de bijbehorende cijfers: aantal getroffen transacties, percentage van het aantal met dezelfde betalingsdienst uitgevoerde betaaltransacties dat door het incident is getroffen, en totale waarde van de transacties. Betalingsdienstaanbieders verstrekken specifieke waarden voor deze variabelen; dit kunnen werkelijke cijfers of schattingen zijn. Entiteiten die melding doen namens verscheidene betalingsdienstaanbieders (geconsolideerde melding) mogen in plaats daarvan bandbreedtes aangeven, waarbij zij de laagste en de hoogste waarden die zijn waargenomen of geschat binnen de groep betalingsdienstaanbieders waarop de melding betrekking heeft, weergeven gescheiden door een liggend streepje. In het algemeen dienen betalingsdienstaanbieders onder 'getroffen transacties' alle binnenlandse en grensoverschrijdende transacties te verstaan die direct of indirect gevolgen ondervinden of waarschijnlijk zullen ondervinden van het incident, en in het bijzonder de transacties die niet konden worden geïnitieerd of verwerkt, de transacties waarvoor de inhoud van het betalingsbericht werd veranderd en de transacties waartoe op frauduleuze wijze opdracht is gegeven (ongeacht de vraag of het geld al dan niet is teruggevorderd). Bovendien dienen betalingsdienstaanbieders als het normale niveau van betalingstransacties te beschouwen het jaargemiddelde van de dagelijkse binnenlandse en grensoverschrijdende betalingstransacties die zijn uitgevoerd met dezelfde betalingsdiensten als die welke door het incident zijn getroffen, met het voorgaande jaar als de referentieperiode voor de berekeningen. Als betalingsdienstaanbieders dit cijfer als niet-representatief beschouwen (bijv. wegens seizoenseffecten), gebruiken zij in plaats daarvan een andere, representatievere maatstaf en verstrekken zij de bevoegde autoriteit de redenen voor deze aanpak in het veld 'Opmerkingen'.

Getroffen betalingsdienstgebruikers: Betalingsdienstaanbieders geven aan welke drempels het incident heeft bereikt of waarschijnlijk zal bereiken, indien van toepassing, evenals de bijbehorende cijfers: totaal aantal betalingsdienstgebruikers dat is getroffen en het percentage van het totale aantal betalingsdienstgebruikers dat is getroffen. Betalingsdienstaanbieders verstrekken concrete waarden voor deze variabelen; dit kunnen werkelijke cijfers of schattingen zijn. Entiteiten die melding doen namens verscheidene betalingsdienstaanbieders (geconsolideerde melding) mogen in plaats daarvan bandbreedtes aangeven, waarbij zij de laagste en de hoogste waarden die zijn waargenomen of geschat binnen de groep betalingsdienstaanbieders waarop de melding betrekking heeft, weergeven gescheiden door een liggend streepje. Betalingsdienstaanbieders verstaan onder ‘getroffen betalingsdienstgebruikers’ alle klanten (uit binnen- en buitenland, zowel consumenten als bedrijven) die een contract hebben met de getroffen betalingsdienstaanbieder op grond waarvan zij toegang hebben tot de getroffen betalingsdienst en de gevolgen van het incident hebben ondervonden of waarschijnlijk zullen ondervinden. Betalingsdienstaanbieders maken gebruik van schattingen op basis van

activiteiten in het verleden om vast te stellen hoeveel betalingsdienstgebruikers tijdens de duur van het incident mogelijk de betalingsdienst hebben gebruikt. In het geval van groepen houdt elke betalingsdienstaanbieder alleen rekening met zijn eigen betalingsdienstgebruikers. Een betalingsdienstaanbieder die operationele diensten aanbiedt aan anderen houdt alleen rekening met de gebruikers van zijn eigen betalingsdienst (indien die er zijn); de betalingsdienstaanbieders die deze operationele diensten ontvangen, beoordelen eveneens het incident met betrekking tot hun eigen betalingsdienstgebruikers. Bovendien beschouwen betalingsdienstaanbieders als het totale aantal betalingsdienstgebruikers het totaalcijfer van betalingsdienstgebruikers in binnen- en buitenland die ten tijde van het incident contractueel aan hen zijn gebonden (of eventueel het meest recente beschikbare cijfer) en die toegang hadden tot de getroffen betalingsdienst, ongeacht hoe groot ze zijn en of zij worden beschouwd als actieve of passieve betalingsdienstgebruikers.

Uitvaltijd dienstverlening: Betalingsdienstaanbieders geven aan of de drempel is of waarschijnlijk zal worden bereikt door het incident, evenals het bijbehorende cijfer: de totale uitvaltijd van de dienstverlening. Betalingsdienstaanbieders verstrekken concrete waarden voor deze variabele; dit kunnen werkelijke cijfers of schattingen zijn. Entiteiten die melding doen namens verscheidene betalingsdienstaanbieders (geconsolideerde melding) mogen in plaats daarvan een bandbreedte aangeven, waarbij zij de laagste en de hoogste waarden die zijn waargenomen of geschat binnen de groep betalingsdienstaanbieders waarop de melding betrekking heeft, weergeven gescheiden door een liggend streepje. Betalingsdienstaanbieders houden rekening met de tijd gedurende welke een taak, proces of kanaal die/dat verband houdt met de levering van betalingsdiensten, niet beschikbaar is of waarschijnlijk niet beschikbaar zal zijn en daarmee (i) het initiëren en/of de uitvoering van een betalingsdienst en/of (ii) de toegang tot een betaalrekening onmogelijk maakt. Betalingsdienstaanbieders tellen de uitvaltijd van de dienstverlening vanaf het moment dat de dienst uitvalt, en zij tellen zowel de perioden mee dat zij open zijn voor de uitvoering van betalingsdiensten als de sluitings- en onderhoudsperioden, voor zover relevant en toepasselijk. Als betalingsdienstaanbieders niet in staat zijn vast te stellen wanneer de uitval is begonnen, rekenen zij de uitvaltijd bij wijze van uitzondering vanaf het moment dat deze aan het licht is gekomen.

Economische gevolgen: Betalingsdienstaanbieders geven aan of de drempel is of waarschijnlijk zal worden bereikt door het incident, evenals de bijbehorende cijfers: de directe en de indirecte kosten. Betalingsdienstaanbieders verstrekken concrete waarden voor deze variabelen; dit kunnen werkelijke cijfers of schattingen zijn. Entiteiten die melding doen namens verscheidene betalingsdienstaanbieders (geconsolideerde meldingen) mogen in plaats daarvan een bandbreedte aangeven, waarbij zij de laagste en de hoogste waarden die zijn waargenomen of geschat binnen de groep betalingsdienstaanbieders waarop de melding betrekking heeft, weergeven gescheiden door een liggend streepje. Betalingsdienstaanbieders houden rekening met zowel de kosten die direct aan het incident kunnen worden gerelateerd als de kosten die indirect met het incident samenhangen. Betalingsdienstaanbieders houden onder meer rekening met onteigend geld of onteigende activa, kosten voor de vervanging van hardware of software, andere forensische of herstelkosten, vergoedingen als gevolg van niet-nakoming van contractuele verplichtingen, sancties, externe verplichtingen en gederfde inkomsten. Wat de indirecte kosten betreft houden betalingsdienstaanbieders alleen rekening met de indirecte kosten die al bekend zijn of waarvan het zeer waarschijnlijk is dat ze zich zullen voordoen.

> **Directe kosten:** hoeveelheid geld (in euro) die het incident direct kost, waaronder geld dat nodig is om het incident te corrigeren (bijv. onteigend geld of onteigende activa, kosten voor de vervanging van hardware en software, vergoedingen als gevolg van niet-nakoming van contractuele verplichtingen).

Indirecte kosten: hoeveelheid geld (in euro) die het incident indirect kost (bijv. schadeloosstellingen/compensaties klanten, gederfde inkomsten door gemiste omzetkansen, mogelijke juridische kosten).

Hoog niveau van interne escalatie: Betalingsdienstaanbieders overwegen of, als gevolg van de impact van het incident op betalingsgerelateerde diensten, de Chief Information Officer (of een persoon in een vergelijkbare functie) al of niet op de hoogte is gesteld of waarschijnlijk zal worden gesteld van het incident buiten een eventuele periodieke kennisgevingsprocedure en op een continue basis tijdens de gehele duur van het incident. In het geval van delegering van meldingen vindt de escalatie plaats binnen de derde partij. Bovendien houden betalingsdienstaanbieders rekening met de vraag of als gevolg van de impact van het incident op betalingsgerelateerde diensten een crisismodus is geïnitieerd of waarschijnlijk zal worden geïnitieerd.

Mogelijke gevolgen voor andere betalingsdienstaanbieders of relevante infrastructuren: betalingsdienstaanbieders beoordelen de impact van het incident op de financiële markt, waarbij onder financiële markt wordt verstaan de financiële-marktinfrastructuren en/of kaartbetalingssystemen die deze en andere betalingsdienstaanbieders ondersteunen. Met name beoordelen betalingsdienstaanbieders of het incident zich heeft herhaald of zich waarschijnlijk zal herhalen bij andere betalingsdienstaanbieders, of het de probleemloze werking van financiële-marktinfrastructuren heeft verstoord of waarschijnlijk zal verstoren en of het de soliditeit van het financiële systeem als geheel in gevaar heeft gebracht of waarschijnlijk in gevaar zal brengen. Betalingsdienstaanbieders houden rekening met diverse aspecten, zoals de vraag of het om een eigen of algemeen verkrijgbare component/software gaat, of het getroffen netwerk intern of extern is en of de betalingsdienstaanbieder in de financiële-marktinfrastructuren waarvan hij lid is, is gestopt of waarschijnlijk zal stoppen met het voldoen aan zijn verplichtingen.

Gevolgen voor de reputatie: Betalingsdienstaanbieders houden rekening met het niveau van zichtbaarheid dat het incident, voor zover hun bekend is, heeft gekregen of waarschijnlijk zal krijgen in de markt. Met name kijken betalingsdienstaanbieders naar de waarschijnlijkheid dat het incident schade zal toebrengen aan de maatschappij, als een goede indicator van het potentieel van het incident om hun reputatie aan te tasten. Betalingsdienstaanbieders houden rekening met de vraag of (i) het incident een zichtbaar proces heeft beïnvloed en daardoor waarschijnlijk aandacht zal krijgen in de media of die aandacht al heeft gekregen (waarbij niet alleen wordt gekeken naar traditionele media zoals kranten, maar ook naar blogs, sociale netwerken, enz.), (ii) wettelijke verplichtingen niet zijn nagekomen of waarschijnlijk niet zullen worden nagekomen, (iii) sancties zijn genegeerd of waarschijnlijk zullen worden genegeerd, of (iv) hetzelfde type incident zich eerder heeft voorgedaan.

B 3 - Beschrijving incident

Soort incident: geef aan of het, voor zover u weet, om een operationeel of een veiligheidsincident gaat.

Operationeel: incident dat voortvloeit uit ontoereikende of falende processen, mensen en systemen of uit overmachtssituaties waardoor de integriteit, beschikbaarheid, vertrouwelijkheid, authenticiteit en/of continuïteit van betalingsgerelateerde diensten wordt beïnvloed.

Veiligheid: ongeautoriseerde toegang tot of gebruik, openbaarmaking, verstoring, wijziging of vernietiging van de activa van de betalingsdienstaanbieder waardoor de integriteit, beschikbaarheid, vertrouwelijkheid, authenticiteit en/of continuïteit van betalingsgerelateerde diensten wordt beïnvloed. Dit kan zich onder meer voordoen wanneer de betalingsdienstaanbieder wordt getroffen door cyberaanvallen, een

ontoereikend opgezet of uitgevoerd veiligheidsbeleid heeft of onvoldoende fysiek beveiligd is.

Oorzaak van incident: geef de oorzaak van het incident aan of, als die nog niet bekend is, de meest waarschijnlijke oorzaak. Er kunnen meerdere antwoorden worden aangevinkt.

In onderzoek: de oorzaak is nog niet vastgesteld.

Externe aanval: de bron van de oorzaak bevindt zich buiten de organisatie en richt zich opzettelijk tegen de betalingsdienstaanbieder (bijv. malware-aanvallen).

Interne aanval: de bron van de oorzaak bevindt zich binnen de organisatie en richt zich opzettelijk tegen de betalingsdienstaanbieder (bijv. interne fraude).

Soort aanval:

Distributed/Denial of Service (D/DoS): een poging om een onlinedienst onbereikbaar te maken door deze te overspoelen met verkeer uit meerdere bronnen.

Infectie van interne systemen: schadelijke activiteit waarbij computersystemen worden aangevallen en wordt geprobeerd schijfruimte of CPU-tijd te stelen, toegang te krijgen tot persoonlijke gegevens, gegevens te corrumperen, spam te sturen naar contacten, enz.

Gerichte inbraak: ongeautoriseerd spioneren en informatie inkijken en stelen via cyberspace.

Andere: elke andere soort aanval waarvan de betalingsdienstaanbieder slachtoffer is geworden, hetzij direct, hetzij via een dienstverlener. Met name als er een aanval is geweest die gericht was op het autorisatie- en authenticatieproces, dient dit vakje te worden aangevinkt. Bijzonderheden worden toegevoegd in het vrijetekstveld.

Externe gebeurtenissen: de oorzaak houdt verband met gebeurtenissen die in het algemeen buiten de controle van de organisatie liggen (bijv. natuurrampen, juridische kwesties, zakelijke kwesties en afhankelijkheden van diensten).

Menselijke fout: het incident werd veroorzaakt door een onopzettelijke fout van een persoon; dit kan een onderdeel zijn van de betalingsprocedure (bijv. het uploaden van het verkeerde batchbestand met betalingen naar het betalingssysteem) of hier op enigerlei wijze mee verbonden zijn (bijv. als de stroom bij vergissing wordt uitgeschakeld en de betalingsactiviteit tot stilstand komt).

Procesfout: de oorzaak van het incident was een slecht ontwerp of een slechte uitvoering van het betaalproces, de procescontroles en/of de ondersteunende processen (zoals het proces voor wijziging/migratie, testen, configuratie, capaciteit, monitoring).

Systeemfout: de oorzaak van het incident houdt verband met ontoereikendheid van het ontwerp, de uitvoering, de componenten, de specificaties, de integratie of de complexiteit van de systemen die de betalingsactiviteit ondersteunen.

Anders: de oorzaak van het incident is geen van de hierboven genoemde. Nadere bijzonderheden worden verstrekt in het vrijetekstveld.

Bent u direct door het incident getroffen of indirect, via een dienstenleverancier?: een incident kan rechtstreeks gericht zijn tegen een betalingsdienstaanbieder of indirect, via een derde, gevolgen voor hem hebben. Geef in het geval van indirecte impact de naam van de dienstverlener(s).

B 4 – Impact van het incident

Getroffen gebouw(en) (adres), indien toepasselijk: als een fysiek gebouw is getroffen, geef dan het adres van dit gebouw.

Getroffen handelskanalen: geef aan welk kanaal of welke kanalen voor interactie met betalingsdienstgebruikers door het incident zijn getroffen. Er kunnen meerdere antwoorden worden aangevinkt.

Bijkantoren: bedrijfsvestigingen (anders dan het hoofdkantoor) die onderdeel zijn van een betalingsdienstaanbieder, geen rechtspersoonlijkheid hebben en direct enkele of alle transacties uitvoeren die inherent zijn aan de activiteit van een betalingsdienstaanbieder. Alle vestigingen van een betalingsdienstaanbieder in eenzelfde lidstaat met het hoofdkantoor in een andere lidstaat worden als één enkel bijkantoor beschouwd.

Elektronisch bankieren: het gebruik van computers om financiële transacties via internet uit te voeren.

Telefonisch bankieren: het gebruik van telefoons om financiële transacties uit te voeren.

Mobiel bankieren: het gebruik van een specifieke bankapplicatie op een smartphone of vergelijkbaar apparaat om financiële transacties uit te voeren.

Geldautomaten: elektromechanische apparaten waarmee betalingsdienstgebruikers contant geld van hun rekening kunnen opnemen en/of toegang kunnen krijgen tot andere diensten.

Verkooppunt: fysiek pand van de handelaar waar de betalingstransactie wordt geïnitieerd.

Anders: het getroffen handelskanaal is geen van de hierboven genoemde. Nadere bijzonderheden worden verstrekt in het vrijetekstveld.

Getroffen betalingsdiensten: geef aan welke betalingsdiensten niet naar behoren functioneren als gevolg van het incident. Er kunnen meerdere antwoorden worden aangevinkt.

Storting van contant geld op een betaalrekening: het overhandigen van contant geld aan een betalingsdienstaanbieder om dit te laten crediteren op een betaalrekening.

Opname van contant geld van een betaalrekening: het verzoek dat een betalingsdienstaanbieder van zijn betalingsdienstgebruiker ontvangt om contant geld te verstrekken en zijn/haar betaalrekening voor datzelfde bedrag te debiteren.

Verrichtingen die vereist zijn voor het beheren van een betaalrekening: de handelingen die moeten worden verricht om een betaalrekening te activeren, te deactiveren en/of in stand te houden (bijv. openen, blokkeren).

Verwerven van betalingsinstrumenten: een betalingsdienst die eruit bestaat dat een betalingsdienstaanbieder met een begunstigde overeenkomt betalingstransacties te accepteren en te verwerken, hetgeen leidt tot een overdracht van geld aan de begunstigde.

Overmakingen: een betalingsdienst voor het crediteren van de betaalrekening van een begunstigde met een betalingstransactie of een reeks betalingstransacties van de betaalrekening van een betaler door een betalingsdienstaanbieder die de betaalrekening van de betaler houdt, op basis van een door de betaler gegeven instructie.

Automatische afschrijvingen: een betalingsdienst voor het debiteren van de betaalrekening van een betaler, waarbij een betalingstransactie wordt geïnitieerd door de begunstigde op basis van de toestemming die de betaler heeft gegeven aan de begunstigde, aan de betalingsdienstaanbieder van de begunstigde of aan de betalingsdienstaanbieder van de betaler zelf.

Kaartbetalingen: een betalingsdienst op basis van de infrastructuur van een betaalkaartsysteem en bedrijfsregels om een betaaltransactie te verrichten met behulp van een kaart, telecommunicatie, een digitaal of IT-apparaat of software, indien deze resulteert in een betaalpas- of creditcardtransactie. Transacties op basis van andere soorten betalingsdiensten behoren niet tot kaartbetalingen.

Uitgifte van betalingsinstrumenten: een betalingsdienst die eruit bestaat dat een betalingsdienstaanbieder met een betaler overeenkomt hem een betalingsinstrument te verstrekken om de betaaltransacties van de betaler te initiëren en te verwerken.

Geldtransfers: een betalingsdienst waarbij geld wordt ontvangen van een betaler zonder dat er betaalrekeningen worden gecreëerd op naam van de betaler of de begunstigde, met als enige doel een corresponderend bedrag over te dragen aan een begunstigde of aan een andere betalingsdienstaanbieder die namens de begunstigde optreedt, en/of waarbij dat geld ontvangen wordt namens en beschikbaar wordt gesteld aan de begunstigde.

Betalingsinitiatiediensten: betalingsdiensten die eruit bestaan dat een betaalopdracht wordt geïnitieerd op verzoek van de betalingsdienstgebruiker met betrekking tot een betaalrekening die wordt gehouden bij een andere betalingsdienstaanbieder.

Rekeninginformatiediensten: online betalingsdiensten die eruit bestaan dat geconsolideerde informatie wordt verstrekt over een of meer betaalrekeningen die de betalingsdienstgebruiker heeft bij een andere betalingsdienstaanbieder of bij verscheidene betalingsdienstaanbieders.

Anders: de getroffen betalingsdienst is geen van de hierboven genoemde. Nadere bijzonderheden worden verstrekt in het vrijetekstveld.

Getroffen functionele gebieden: geef aan welke stap of stappen van het betaalproces door het incident zijn getroffen. Er kunnen meerdere antwoorden worden aangevinkt.

Authenticatie/autorisatie: procedures die de betalingsdienstaanbieder in staat stellen de identiteit van een betalingsdienstgebruiker of de validiteit van het gebruik van een specifiek betalingsinstrument te verifiëren, met inbegrip van het gebruik van de persoonlijke aanmeldgegevens van de gebruiker en de toestemming van de betalingsdienstgebruiker (of een derde die namens die gebruiker handelt) om geld of effecten over te boeken.

Communicatie: informatiestroom ten behoeve van identificatie, authenticatie, kennisgeving en informatie tussen de betalingsdienstaanbieder die de rekening beheert en aanbieders van betalingsinitiatiediensten, aanbieders van rekeninginformatiediensten, betalers, begunstigden en andere betalingsdienstaanbieders.

Clearing: het proces van het verzenden, reconciliëren en in sommige gevallen bevestigen van overboekingsopdrachten voorafgaand aan de afwikkeling, mogelijk met inbegrip van de saldering van opdrachten en de vaststelling van eindposities voor afwikkeling.

Directe afwikkeling: de voltooiing van een transactie of een verwerking met het doel de verplichtingen van deelnemers te vervullen door de overdracht van geld, wanneer deze handeling door de getroffen betalingsdienstaanbieder zelf wordt uitgevoerd.

Indirecte afwikkeling: de voltooiing van een transactie of een verwerking met het doel de verplichtingen van deelnemers te vervullen door de overdracht van geld, wanneer deze handeling door een andere betalingsdienstaanbieder namens de getroffen betalingsdienstaanbieder wordt uitgevoerd.

Anders: het getroffen functionele gebied is geen van de hierboven genoemde. Nadere bijzonderheden worden verstrekt in het vrijetekstveld.

Getroffen systemen en componenten: geef aan welk deel of welke delen van de technische infrastructuur van de betalingsdienstaanbieder door het incident zijn getroffen. Er kunnen meerdere antwoorden worden aangevinkt.

Applicatie/software: programma's, besturingssystemen, enz. die de levering van betalingsdiensten door de betalingsdienstaanbieder ondersteunen.

Database: datastructuur waarin persoonlijke informatie en betaalinformatie wordt opgeslagen die nodig is om betalingstransacties uit te voeren.

Hardware: fysieke technische apparatuur waarop de processen worden uitgevoerd en/of de gegevens worden opgeslagen die betalingsdienstaanbieders nodig hebben om hun betalingsgerelateerde activiteiten te verrichten.

Netwerk/infrastructuur: openbare of privé-telecommunicatienetwerken die de uitwisseling van gegevens en informatie tijdens het betalingsproces mogelijk maken (bijv. internet).

Anders: het getroffen systeem of de getroffen component is geen van de hierboven genoemde. Nadere bijzonderheden worden verstrekt in het vrijetekstveld.

Getroffen medewerkers: geef aan of het incident gevolgen heeft gehad voor de medewerkers van de betalingsdienstaanbieder en zo ja, licht dit toe in het vrijetekstveld.

B 5 – Beperking van het incident

Welke acties/maatregelen zijn tot nu toe genomen of gepland om van het incident te herstellen? Geef bijzonderheden over acties die zijn ondernomen of gepland om het incident voorlopig aan te pakken.

Zijn het bedrijfscontinuïteitsplan en/of het uitwijkplan geactiveerd? Geef aan of dit is gebeurd en zo ja, vermeld de meest relevante bijzonderheden over wat er is gebeurd (wanneer ze zijn geactiveerd en wat deze plannen inhielden).

Heeft de betalingsdienstaanbieder sommige controles opgeschort of versoepeld wegens het incident? Geef aan of de betalingsdienstaanbieder sommige controles terzijde heeft moeten schuiven (bijv. niet langer het vier-ogenprincipe hanteren) om het incident aan te pakken, en zo ja, geef bijzonderheden over de onderliggende redenen die het opschorten of versoepelen van controles rechtvaardigen.

C – Eindmelding

C 1 – Algemene informatie

Update van de informatie in de tussentijdse melding (samenvatting): geef nadere informatie over de acties die zijn ondernomen om van het incident te herstellen en herhaling te voorkomen, de analyse van de onderliggende oorzaak, getrokken lessen, enz.

Datum en tijdstip van sluiting van het incident: vermeld de datum en het tijdstip waarop het incident als gesloten werd beschouwd.

Zijn de oorspronkelijke controles weer van kracht? Geef, als de betalingsdienstaanbieder bepaalde controles heeft opgeschort of versoepeld wegens het incident, aan of die controles weer van kracht zijn; aanvullende informatie kan worden ingevuld in het vrijetekstveld.

C 2 – Analyse onderliggende oorzaak en opvolging

Wat was de onderliggende oorzaak (indien al bekend)? Leg uit wat de onderliggende oorzaak van het incident is of, als die nog niet bekend is, welke voorlopige conclusies kunnen worden getrokken uit de analyse van de onderliggende oorzaak. Betalingsdienstaanbieders kunnen, als ze dit nodig achten, een bestand met gedetailleerde informatie bijvoegen.

Belangrijkste corrigerende acties/maatregelen die zijn genomen of gepland om te voorkomen dat het incident in de toekomst opnieuw voorkomt, indien deze al bekend zijn: beschrijf de belangrijkste acties die zijn ondernomen of gepland om te voorkomen dat het incident in de toekomst opnieuw voorkomt.

C 3 – Aanvullende informatie

Is het incident ter informatie gedeeld met andere betalingsdienstaanbieders? Geef een overzicht van de betalingsdienstaanbieders waarmee - formeel of informeel - contact is opgenomen om het incident met hen te bespreken en geef daarbij bijzonderheden over de betalingsdienstaanbieders die zijn geïnformeerd, de informatie die is gedeeld en de onderliggende redenen voor het delen van deze informatie.

Zijn er gerechtelijke stappen ondernomen tegen de betalingsdienstaanbieder? Geef aan of er, als gevolg van het incident, op het moment van het invullen van de eindmelding, juridische stappen zijn genomen tegen de betalingsdienstaanbieder (bijv. of hij voor de rechter is gedaagd of zijn vergunning is kwijtgeraakt) als gevolg van het incident.