EBA/GL/2021/03

10 juni 2021

Herziene richtsnoeren

voor de melding van grote incidenten uit hoofde van PSD2

1. Nalevings- en rapportageverplichtingen

Status van deze richtsnoeren

1. Dit document bevat richtsnoeren die zijn uitgebracht op grond van artikel 16 van de EBA-verordening[1]. Overeenkomstig artikel 16, lid 3, van de EBA-verordening moeten bevoegde autoriteiten en financiële instellingen zich tot het uiterste inspannen om aan de richtsnoeren te voldoen.

2. Richtsnoeren geven weer wat in de opvatting van 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 de EBA-verordening 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 de EBA-verordening stellen de bevoegde autoriteiten EBA vóór (07.11.2021) ervan in kennis of zij aan deze richtsnoeren voldoen of voornemens zijn deze op te volgen, of geven zij, indien dit niet het geval is, aan waarom zij hier niet aan voldoen of niet voornemens zijn deze op te volgen. Bevoegde autoriteiten die bij het verstrijken van de termijn niet hebben gereageerd, worden geacht niet aan de richtsnoeren te hebben voldaan. Kennisgevingen worden ingediend door het formulier op de EBA-website te versturen onder vermelding van het kenmerk ‘EBA/GL/2021/03’. 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 de website van EBA 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 (tweede richtlijn betalingsdiensten, PSD2).

6. Deze richtsnoeren verschaffen met name de criteria voor de classificatie van grote operationele en beveiligingsincidenten 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 PSD2.

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 PSD2, 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 beveiligingsincidenten overeenkomstig artikel 96 van PSD2.

10. Deze richtsnoeren gelden voor alle incidenten die onder de definitie vallen van ‘groot operationeel of beveiligingsincident’; 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 beveiligingsincident 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.

12. Deze richtsnoeren gelden ook voor grote incidenten die functies treffen die door betalingsdienstaanbieders zijn uitbesteed aan derde partijen.

Geadresseerden

13. De eerste reeks richtsnoeren (hoofdstuk 4) is gericht tot betalingsdienstaanbieders als gedefinieerd in artikel 4, lid 11, van PSD2 en vermeld in artikel 4, lid 1, van Verordening (EU) nr. 1093/2010.

14. 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

15. Tenzij anders aangegeven, hebben de termen die in PSD2 worden gebruikt en gedefinieerd in deze richtsnoeren dezelfde betekenis. In deze richtsnoeren gelden daarnaast de volgende definities:

Operationeel of beveiligingsincident	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 en/of authenticiteit van betalingsgerelateerde diensten.
Integriteit	De eigenschap dat de juistheid en de volledigheid van activa (waaronder gegevens) worden gewaarborgd.
Beschikbaarheid	De eigenschap van betalingsgerelateerde diensten dat ze volledig toegankelijk zijn voor betalingsdienstgebruikers en door hen kunnen worden gebruikt, op vooraf door de betalingsdienstaanbieder vastgelegde aanvaardbare niveaus.
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.

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

16. Deze richtsnoeren gelden vanaf 1 januari 2022.

Intrekking

17. De volgende richtsnoeren worden met ingang van 1 januari 2022 ingetrokken:

Richtsnoeren voor de melding van grote incidenten uit hoofde van Richtlijn (EU) 2015/2366 (tweede richtlijn betalingsdiensten, PSD2) (EBA/GL/2017/10)

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

Richtsnoer 1: Classificatie als groot incident

1.1. Betalingsdienstaanbieders classificeren operationele of beveiligingsincidenten 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 beveiligingsincident 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. Inbreuk op de beveiliging van netwerk- of informatiesystemen

Betalingsdienstaanbieders bepalen of een kwaadwillige handeling de beveiliging van netwerk- of informatiesystemen die verband houden met de levering van betalingsdiensten heeft gecompromitteerd.

iv. Uitvaltijd dienstverlening

Betalingsdienstaanbieders bepalen de tijdsduur gedurende welke de dienst waarschijnlijk niet beschikbaar zal zijn voor de gebruiker van de betalingsdienst, of gedurende welke de betalingsopdracht – in de zin van artikel 4, lid 13, van PSD2 – niet kan worden uitgevoerd door de betalingsdienstaanbieder.

v. 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).

vi. Hoog niveau van interne escalatie

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

vii. 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, financiëlemarktinfrastructuren en/of betalingssystemen.

viii. 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) of waarvan de juiste uitvoering op een andere manier door het incident wordt verhinderd of belemmerd.

Voor operationele incidenten die van invloed zijn op het vermogen om transacties te initiëren en/of te verwerken, melden betalingsdienstaanbieders alleen de incidenten die langer dan één uur duren. De duur van het incident wordt gemeten vanaf het moment waarop het incident zich voordoet, tot het moment waarop de reguliere activiteiten/verrichtingen zodanig zijn hersteld dat zij plaatsvinden op hetzelfde dienstverleningsniveau als vóór het incident.

Daarnaast beschouwen betalingsdienstaanbieders als het normale niveau van betalingstransacties de dagelijkse binnenlandse en grensoverschrijdende betalingstransacties gemiddeld over een jaar 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 de bijlage).

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 hun 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.

Voor operationele incidenten die van invloed zijn op het vermogen om transacties te initiëren en/of te verwerken, melden betalingsdienstaanbieders alleen de incidenten die betalingsdienstgebruikers treffen en langer dan één uur duren. De duur van het incident wordt gemeten vanaf het moment waarop het incident zich voordoet, tot het moment waarop de reguliere activiteiten/verrichtingen zodanig zijn hersteld dat zij plaatsvinden op hetzelfde dienstverleningsniveau als vóór het incident.

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. Inbreuk op de beveiliging van netwerk- of informatiesystemen

Betalingsdienstaanbieders bepalen of een kwaadwillige handeling de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van netwerk- of informatiesystemen (met inbegrip van gegevens) die verband houden met de levering van betalingsdiensten heeft gecompromitteerd.

iv. 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. 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 is gedetecteerd.

v. 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.

vi. *Hoog niveau van interne escalatie*

Betalingsdienstaanbieders houden rekening met de vraag of, als gevolg van de impact van het incident op betalingsgerelateerde diensten, het leidinggevend orgaan als gedefinieerd door de EBA-richtsnoeren inzake ICT en risicobeheer op het gebied van beveiliging al of niet, overeenkomstig richtsnoer 60, letter d), van deze richtsnoeren, 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.

vii. *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 betalingssystemen die hen en de overige 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.

viii. *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) betalingsdienstgebruikers en/of andere betalingsdienstaanbieders hebben geklaagd over het nadelige effect van het incident, ii) het incident gevolgen heeft gehad voor een zichtbaar betalingsdienstgerelateerd 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 blogs, sociale netwerken, enz.), iii) contractuele verplichtingen niet zijn nagekomen of waarschijnlijk niet zullen worden nagekomen, met als gevolg de publicatie van gerechtelijke stappen tegen de betalingsdienstaanbieder, iv) wettelijke voorschriften niet zijn nageleefd, met als gevolg de oplegging van toezichtmaatregelen of sancties die openbaar zijn gemaakt of waarschijnlijk openbaar zullen worden gemaakt, en v) of zich eerder een vergelijkbaar incident 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** duur van het incident > 1 uur* **of** > 500 000 EUR **en** duur van het incident > 1 uur*	> 25 % van het normale aantal transacties van de betalingsdienstaanbieder **of** > 15 000 000 EUR
Getroffen betalingsdienstgebruikers	> 5 000 **en** duur van het incident > 1 uur* **of** > 10 % van de gebruikers van de betalingsdiensten van de aanbieder **en** duur van het incident > 1 uur*	> 50 000 **of** > 25 % van de gebruikers van de betalingsdiensten van de aanbieder
Uitvaltijd dienstverlening	> 2 uur	Niet van toepassing
Inbreuk op de beveiliging van netwerk- of informatiesystemen	Ja	Niet van toepassing
Economische gevolgen	Niet van toepassing	> Max (0,1 % tier 1-kapitaal**, 200 000 EUR) **of**

		> 5 000 000 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

* De drempel van meer dan één uur voor de duur van het incident geldt alleen voor operationele incidenten die van invloed zijn op het vermogen van de betalingsdienstaanbieder om transacties te initiëren of te verwerken.

**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. Elke herclassificatie van het incident van groot naar niet-groot wordt overeenkomstig richtsnoer 2.21 en onverwijld aan de bevoegde autoriteit meegedeeld.

Richtsnoer 2: Meldingsproces

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

2.2. Betalingsdienstaanbieders gebruiken en hetzelfde formulier wanneer zij de initiële melding, de tussentijdse melding en de eindmelding met betrekking tot het incident indienen. Betalingsdienstaanbieders vullen stapsgewijs één formulier in en werken, waar van toepassing, de daarin bij eerdere meldingen verstrekte informatie bij.

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 als voorzien in artikel 96, lid 1, tweede alinea, van PSD2, zodra deze beschikbaar is.

2.4. Betalingsdienstaanbieders verstrekken op verzoek van de bevoegde autoriteit in de lidstaat van herkomst aanvullende documenten die de in het gestandaardiseerde formulier

verstrekte informatie completeren. 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.

2.5. Alle aanvullende informatie in de documenten die door betalingsdienstaanbieders aan de bevoegde autoriteit wordt verstrekt, hetzij op initiatief van de betalingsdienstaanbieder hetzij op verzoek van de bevoegde autoriteit overeenkomstig richtsnoer 2.4, wordt door de betalingsdienstaanbieder in het in richtsnoer 2.1 bedoelde formulier vermeld.

2.6. Betalingsdienstaanbieders waarborgen te allen tijde de vertrouwelijkheid en de integriteit van de informatie die zij uitwisselen en hun correcte authenticatie tegenover de bevoegde autoriteit in hun lidstaat van herkomst.

Initiële melding

2.7. Betalingsdienstaanbieders dienen bij de bevoegde autoriteit in hun lidstaat van herkomst een initiële melding in nadat een operationeel of beveiligingsincident als groot is geclassificeerd. Bevoegde autoriteiten bevestigen onverwijld de ontvangst van de initiële melding en kennen een unieke referentiecode als eenduidige identificatie van het incident toe. Betalingsdienstaanbieders vermelden deze referentiecode wanneer zij een bijwerking van de initiële melding of van de tussentijdse melding(en) of eindmelding van hetzelfde incident indienen, tenzij de tussentijdse melding(en) en eindmelding gezamenlijk met de initiële melding worden ingediend.

2.8. Betalingsdienstaanbieders sturen de initiële melding naar de bevoegde autoriteit binnen vier uur na het moment waarop het operationele of beveiligingsincident als groot is geclassificeerd. Als bekend is dat de meldingskanalen van de bevoegde autoriteit op dat tijdstip niet beschikbaar of niet operationeel zijn, sturen betalingsdienstaanbieders de initiële melding zodra deze kanalen weer beschikbaar/operationeel zijn.

2.9. Betalingsdienstaanbieders classificeren het incident overeenkomstig richtsnoer 1.1 en richtsnoer 1.4 bijtijds nadat het incident is ontdekt, maar niet later dan 24 uur na de ontdekking van het incident, en zonder onnodige vertraging nadat de voor de classificatie van het incident vereiste informatie voor de betalingsdienstaanbieder beschikbaar is gekomen. Als meer tijd nodig is om het incident te classificeren, lichten betalingsdienstaanbieders de redenen hiervoor toe in de bij de bevoegde autoriteit in te dienen initiële melding.

2.10. Betalingsdienstaanbieders dienen ook een initiële melding in bij de bevoegde autoriteit in de lidstaat van herkomst wanneer een incident dat eerder niet groot was, wordt geherclassificeerd als een groot incident. 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.

2.11. Betalingsdienstaanbieders verstrekken kerngegevens in hun initiële melding (d.w.z. rubriek A van het formulier); zij vermelden enkele basiskenmerken van het incident en de voorziene gevolgen ervan op basis van de informatie die onmiddellijk beschikbaar is nadat het incident is geclassificeerd als groot. Betalingsdienstaanbieders maken gebruik van schattingen wanneer er geen werkelijke gegevens beschikbaar zijn.

Tussentijdse melding

2.12. Wanneer de reguliere activiteiten zijn hersteld en de situatie is genormaliseerd, dienen betalingsdienstaanbieders de tussentijdse melding in waarin ze de bevoegde autoriteit hiervan op de hoogte stellen. Betalingsdienstaanbieders beschouwen de situatie als weer normaal wanneer de activiteiten weer plaatsvinden op hetzelfde dienstverleningsniveau en/of onder dezelfde omstandigheden als gedefinieerd door de betalingsdienstaanbieder of als extern vastgelegd in een Service Level Agreement (verwerkingstijden, capaciteit, beveiligingsvereisten, enz.), en als er geen noodmaatregelen meer van kracht zijn. De tussentijdse melding bevat een gedetailleerdere beschrijving van het incident en de gevolgen daarvan (rubriek B van het formulier).

2.13. Indien de reguliere activiteiten nog niet zijn hersteld, dienen betalingsdienstaanbieders bij de bevoegde autoriteit binnen drie werkdagen na indiening van de initiële melding een tussentijdse melding in.

2.14. Betalingsdienstaanbieders werken de informatie die al verstrekt is in de rubrieken A en B van het formulier bij wanneer zij kennis krijgen van significante veranderingen sinds de indiening van 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). Dit geldt ook wanneer het incident niet binnen drie werkdagen is opgelost, in welk geval betalingsdienstaanbieders een aanvullende tussentijdse melding moeten indienen. Betalingsdienstaanbieders stellen in ieder geval een tussentijdse melding op wanneer de bevoegde autoriteit in de lidstaat van herkomst daarom verzoekt.

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

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

Eindmelding

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

2.18. Betalingsdienstaanbieders sturen de eindmelding binnen twintig werkdagen 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 of de onderliggende oorzaken nog niet zijn vastgesteld), 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 vier uur sinds het incident werd geclassificeerd als groot, streven zij ernaar alle informatie voor de initiële, de tussentijdse en de eindmelding samen in te dienen.

2.20. Betalingsdienstaanbieders nemen in hun eindmelding volledige informatie op, 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 in elk geval binnen de termijn voor de indiening van 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 is geherclassificeerd.

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 delegatie 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 delegatie 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 EBA-richtsnoeren inzake uitbesteding (EBA/GL/2019/02) met betrekking tot alle betalingsdienstaanbieders.

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 zijn 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 beveiligingsincident), stellen de bevoegde autoriteit in de lidstaat van herkomst hiervan in kennis, verstrekken 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 een lijst verstrekt van alle betalingsdienstaanbieders die door het incident zijn getroffen.

e. 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.

f. 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 van het formulier), de derde partij ofwel i) deze apart invult voor elke getroffen betalingsdienstaanbieder, waarbij hij specificeert op welke betalingsdienstaanbieder de informatie betrekking heeft, ofwel ii) de cumulatieve waarden gebruikt die zijn vastgesteld of geschat voor de betalingsdienstaanbieders.

g. De derde partij houdt de betalingsdienstaanbieder te allen tijde op de hoogte 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 mogelijk is zonder de vertrouwelijkheid van de informatie met betrekking tot andere betalingsdienstaanbieders te schenden.

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 delegatie 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 beveiligingsincident overeenkomstig artikel 96 van PSD2 en deze richtsnoeren, dienen betalingsdienstaanbieders hun meldingsverplichtingen te vervullen 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.

3.6. Betalingsdienstaanbieders waarborgen dat, wanneer een incident is veroorzaakt door een verstoring van de door een technische-dienstverlener geleverde diensten (of een infrastructuur) die meerdere betalingsdienstaanbieders treft, de gedelegeerde melding betrekking heeft op de individuele gegevens van de betalingsdienstaanbieder (behalve in geval van geconsolideerde meldingen).

Richtsnoer 4: Operationeel en beveiligingsbeleid

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 beveiligingsbeleid.

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 beveiligingsincident 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 beveiligingsincidenten aan de binnenlandse autoriteiten die zijn vastgesteld na de toepassing van richtsnoer 5.1, 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 (d.w.z. de tussentijdse melding).

6.2. Bevoegde autoriteiten verstrekken de 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 verstrekt in de volgende velden van het formulier (ofwel in de initiële melding, ofwel in de tussentijdse melding):

- datum en tijdstip van classificatie van het incident als groot;
- datum en tijdstip van 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 de relevante binnenlandse autoriteiten. Bevoegde autoriteiten verstrekken echter wel de naam en het adres van de meldende betalingsdienstaanbieder aan de 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 en hun correcte authenticatie tegenover de relevante binnenlandse autoriteiten. 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.

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 beveiligingsincident, door gebruik te maken van een gestandaardiseerd bestand dat beschikbaar is op de website van EBA.

Richtsnoer 8: Communicatie

8.1. Bevoegde autoriteiten waarborgen te allen tijde de vertrouwelijkheid en de integriteit van de informatie die zij opslaan en delen, en hun correcte authenticatie 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 – Formulier voor meldingen door betalingsdienstaanbieders

Initiële melding

Initiële melding	binnen vier uur na classificatie van het incident als groot		Reset selecties vervolgkeuzelijsten
Datum melding *(DD/MM/JJJJ)*		Tijdstip *(UU:MM)*	
Referentiecode incident			

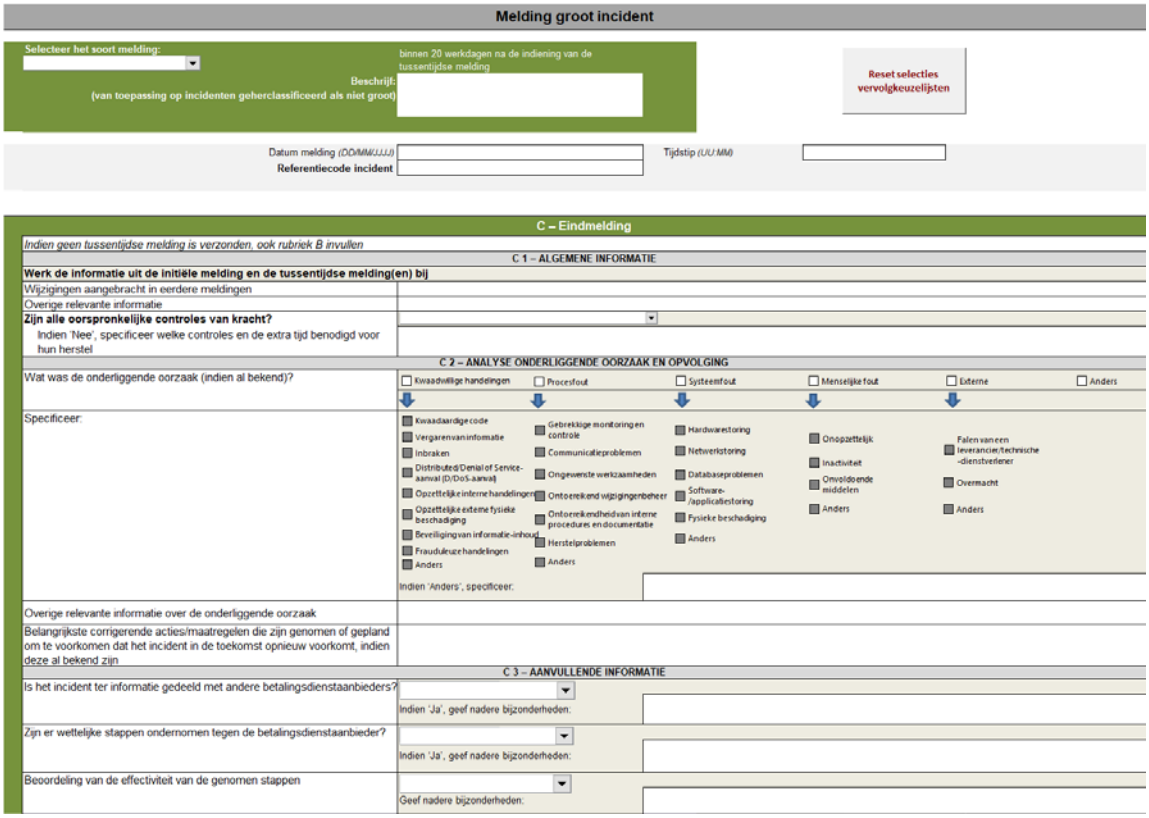
A – Initiële melding						
A 1 – ALGEMENE INFORMATIE						
Soort melding						
Soort melding						
Getroffen betalingsdienstaanbieder (BDA)						
Naam betalingsdienstaanbieder						
Nationaal identificatienummer betalingsdienstaanbieder						
Hoofd van groep, indien van toepassing						
Door het incident getroffen land(en)	☐ 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
Eerste contactpersoon		E-mail		Telefoon		
Tweede contactpersoon		E-mail		Telefoon		
Meldende entiteit (vul dit gedeelte in als de meldende entiteit niet de getroffen betalingsdienstaanbieder is in het geval van delegering van meldingen)						
Naam van de meldende entiteit						
Nationaal identificatienummer						
Eerste contactpersoon		E-mail		Telefoon		
Tweede contactpersoon		E-mail		Telefoon		
A 2 – ONTDEKKING INCIDENT en CLASSIFICATIE						
Datum en tijdstip van de ontdekking van het incident *(DD/MM/JJJJ UU:MM)*						
Datum en tijdstip van de classificatie van het incident *(DD/MM/JJJJ UU:MM)*						
Het incident is ontdekt door		Indien 'Anders', gelieve te specificeren:				
Soort incident						
Criteria die aanleiding geven tot melding van groot incident	☐ Getroffen transacties ☐ Getroffen betalingsdienstgebruike ☐ Uitval tijd dienstverlening ☐ Schending van de beveiliging van netwerk- of informatiesystemen ☐ Economische gevolgen ☐ Hoog niveau van interne escalatie ☑ Mogelijke gevolgen voor andere BDA's of relevante infrastructuren ☐ Gevolgen voor de reputatie					
Korte, algemene beschrijving van het incident						
Impact in andere EU-lidstaten, indien van toepassing						
Melding aan andere autoriteiten		Indien 'Ja', gelieve te specificeren:				
Redenen voor late indiening van de initiële melding						

Tussentijdse melding

Melding groot incident			
Tussentijdse melding	uiterlijk 3 werkdagen na de indiening van de initiële melding		Reset selecties vervolgkeuzelijsten
Datum melding *(DD/MM/JJJJ)*		Tijdstip *(UU:MM)*	
Referentiecode incident			

B – Tussentijdse melding			
B 1 – ALGEMENE INFORMATIE			
Gedetailleerdere beschrijving van het incident:			
Wat is het specifieke probleem?			
Hoe is het incident begonnen?			
Hoe heeft het zich ontwikkeld?			
Wat zijn de gevolgen (in het bijzonder voor betalingsdienstgebruikers)?			
Zijn betalingsdienstgebruikers op de hoogte gesteld van het incident?		Indien 'Ja', gelieve te specificeren:	
Hield het incident verband met een of meer eerdere incidenten?		Indien 'Ja', gelieve te specificeren:	
Zijn andere dienstverleners/derde partijen getroffen of bij het incident betrokken?		Indien 'Ja', gelieve te specificeren:	
Is crisismanagement gestart (intern of extern)?		Indien 'Ja', gelieve te specificeren:	
Datum en tijdstip van het begin van het incident (indien al vastgesteld) *(DD/MM/JJJJ UU:MM)*			
Datum en tijdstip waarop het incident is hersteld of naar verwachting zal zijn hersteld *(DD/MM/JJJJ UU:MM)*			
Getroffen functionele gebieden	☐ Authenticatie/autorisatie ☐ Directe afwikkeling ☐ Communicatie ☐ Indirecte afwikkeling ☐ Clearing ☐ Anders	Indien 'Anders', gelieve te specificeren:	
Wijzigingen aangebracht in eerdere meldingen			
B 2 – CLASSIFICATIE INCIDENT/INFORMATIE OVER HET INCIDENT			
Getroffen transacties[2]	Impactniveau Aantal getroffen transacties Als percentage van normale aantal transacties Waarde van getroffen transacties in EUR Duur van het incident (alleen van toepassing voor operationele incidenten) Opmerkingen:		
Getroffen betalingsdienstgebruikers[3]	Impactniveau Aantal getroffen betalingsdienstgebruikers Als percentage van totale aantal betalingsdienstgebruik		
Schending van de beveiliging van netwerk- of informatiesystemen	Beschrijf hoe de netwerk- of informatiesystemen zijn getroffen		
Uitvaltijd dienstverlening	Totale uitvaltijd dienstverlening: Dagen: Uren: Minuten:		
Economische gevolgen	Impactniveau Directe kosten in EUR Indirecte kosten in EUR		
Hoog niveau van interne escalatie	Beschrijf het niveau van interne escalatie van het incident, en geef aan of hierdoor een crisismodus (of een vergelijkbare modus) is geïnitieerd of waarschijnlijk zal worden geïnitieerd, en, indien dat zo is, specificeer		
Mogelijke gevolgen voor andere BDA's of relevante infrastructuren	Beschrijf hoe dit incident gevolgen zou kunnen hebben voor andere betalingsdienstaanbieders en/of infrastructuren		
Gevolgen voor de reputatie	Beschrijf hoe het incident gevolgen zou kunnen hebben voor de reputatie van de betalingsdienstaanbieder (bijv. media-aandacht, publicatie van gerechtelijke stappen of overtreding van wet- of regelgeving, enz.)		
B 3 – BESCHRIJVING INCIDENT			
Soort incident			
Oorzaak van incident	☐ In onderzoek ☐ Kwaadwillige handelingen ☐ Procesfout ☐ Systeemfout ☐ Menselijke fouten ☐ Externe gebeurtenissen ☐ Anders	Indien 'Anders', specificeer:	
Bent u direct door het incident getroffen, of indirect via een dienstverlener?		Indien 'Indirect', geef de naam van de dienstverlener:	
B 4 – IMPACT VAN HET INCIDENT			
Totale impact	☐ Integriteit ☐ Beschikbaarheid ☐ Vertrouwelijkheid ☐ Authenticiteit		
Getroffen handelskanalen	☐ Bijkantoren ☐ Telefonisch bankieren ☐ Verkooppunt ☐ Elektronisch bankieren ☐ Mobiel bankieren ☐ Anders ☐ Elektronische handel (e-handel) ☑ Geldautomaten		
	Indien 'Anders', specificeer:		
Getroffen betalingsdiensten	☐ Storting van contant geld op een betaalrekening ☐ Opname van contant geld van een betaalrekening ☐ Verrichtingen die vereist zijn voor het beheren van een ☐ Verwerven van betalingsinstrumenten ☐ Overmakingen ☐ Automatische afschrijvingen ☐ Kaartbetalingen ☐ Uitgifte van betalingsinstrumenten ☐ Geldtransfers ☐ Betalingsinitiatiedi ☐ Rekeninginformatiediensten		
B 5 – BEPERKING VAN HET INCIDENT			
Welke acties/maatregelen zijn tot nu toe genomen of gepland om van het incident te herstellen?			
Zijn het bedrijfscontinuïteitsplan en/of het uitwijkplan geactiveerd?			
Indien ja, wanneer? *(DD/MM/JJJJ UU:MM)*			
Indien ja, specificeer			

Eindmelding



Melding groot incident

Selecteer het soort melding:

binnen 20 werkdagen na de indiening van de tussentijdse melding

Beschrijf: (van toepassing op incidenten geherclassificeerd als niet groot)

Reset selecties vervolgkeuzelijsten

Datum melding (DD/MM/JJJJ)

Tijdstip (UU:MM)

Referentiecode incident

C – Eindmelding

Indien geen tussentijdse melding is verzonden, ook rubriek B invullen

C 1 – ALGEMENE INFORMATIE

Werk de informatie uit de initiële melding en de tussentijdse melding(en) bij

Wijzigingen aangebracht in eerdere meldingen

Overige relevante informatie

Zijn alle oorspronkelijke controles van kracht?

Indien 'Nee', specificeer welke controles en de extra tijd benodigd voor hun herstel

C 2 – ANALYSE ONDERLIGGENDE OORZAAK EN OPVOLGING

Wat was de onderliggende oorzaak (indien al bekend)?

☐ Kwaadwillige handelingen ☐ Procesfout ☐ Systeemfout ☐ Menselijke fout ☐ Externe ☐ Anders

Specificeer:

- Kwaadaardige code
- Vergaren van informatie
- Inbraken
- Distributed/Denial of Service-aanval (D/DoS-aanval)
- Opzettelijke interne handelingen
- Opzettelijke externe fysieke beschadiging
- Beveiliging van informatie-inhoud
- Fraudeuze handelingen
- Anders

- Gebrekkige monitoring en controle
- Communicatieproblemen
- Ongewenste werkzaamheden
- Ontoereikend wijzigingenbeheer
- Ontoereikendheid van interne procedures en documentatie
- Herstelproblemen
- Anders

- Hardwarestoring
- Netwerkstoring
- Databaseproblemen
- Software-/applicatiestoring
- Fysieke beschadiging
- Anders

- Onopzettelijk
- Inactiviteit
- Onvoldoende middelen
- Anders

- Falen van een leverancier/technische -dienstverlener
- Overmacht
- Anders

Indien 'Anders', specificeer:

Overige relevante informatie over de onderliggende oorzaak

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

C 3 – AANVULLENDE INFORMATIE

Is het incident ter informatie gedeeld met andere betalingsdienstaanbieders?

Indien 'Ja', geef nadere bijzonderheden:

Zijn er wettelijke stappen ondernomen tegen de betalingsdienstaanbieder?

Indien 'Ja', geef nadere bijzonderheden:

Beoordeling van de effectiviteit van de genomen stappen

Geef nadere bijzonderheden:

AANWIJZINGEN VOOR HET INVULLEN VAN HET FORMULIER

Betalingsdienstaanbieders (BDA's) 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. Betalingsdienstaanbieders gebruiken hetzelfde formulier wanneer zij de initiële melding, de tussentijdse melding(en) en de eindmelding van hetzelfde incident indienen. 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: deze bevat een gedetailleerdere beschrijving van het incident en de gevolgen daarvan. Het is een update van de initiële melding (en van een eerdere tussentijdse melding, indien van toepassing) over hetzelfde incident.

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 en moet worden geherclassificeerd.

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 voor deze herclassificatie zijn.

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

Referentiecode incident (toepasselijk voor tussentijdse meldingen en de eindmelding en voor updates van de initiële melding): de referentiecode die op het moment van de initiële melding door de bevoegde autoriteit is verstrekt als eenduidige identificatie van het incident. Elke bevoegde autoriteit voegt als prefix de tweecijferige ISO-code[2] van haar respectieve lidstaat toe.

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 binnen dezelfde lidstaat die getroffen zijn door hetzelfde grote operationele of beveiligingsincident en gebruikmaken van de mogelijkheid van geconsolideerde meldingen. De velden onder 'Getroffen betalingsdienstaanbieder (BDA)' 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 (BDA): 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.

Nationaal identificatienummer betalingsdienstaanbieder: het unieke nationale identificatienummer dat door de bevoegde autoriteit in de lidstaat van herkomst in haar nationale register wordt gebruikt om de betalingsdienstaanbieder eenduidig te identificeren.

[2] Zie de alpha-2 landcodes volgens ISO-3166 op https://www.iso.org/iso-3166-country-codes.html

Hoofd van groep: geef in het geval van groepen entiteiten als gedefinieerd in artikel 4, lid 40, van PSD2 de naam van de hoofdentiteit op.

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), ongeacht de ernst van het incident in het andere land/de andere landen. 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, in het geval een derde dienstaanbieder 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 terrein.

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

Telefoon: telefoonnummer dat kan 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 kan opnemen bij vragen over een incident, wanneer de eerste contactpersoon niet beschikbaar is. In het geval een derde dienstaanbieder de melding doet namens de getroffen betalingsdienstaanbieder, voor- en achternaam van een alternatieve persoon van de afdeling incidentbeheer/risicobeheer of een soortgelijk terrein 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 dat kan 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, indien van toepassing.

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

Nationaal identificatienummer: het unieke nationale identificatienummer dat wordt gebruikt in het land waar de derde partij is gevestigd, om de entiteit die het incident meldt, eenduidig te identificeren. Als de meldende derde partij een betalingsdienstaanbieder is, is het nationale identificatienummer het unieke nationale identificatienummer van de betalingsdienstaanbieder dat door de bevoegde autoriteit in de lidstaat van herkomst in haar nationale register wordt gebruikt.

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

A 2 - Ontdekking incident en classificatie

Datum en tijdstip van de ontdekking van het incident: de datum en het tijdstip waarop het incident voor het eerst is vastgesteld.

Datum en tijdstip van de classificatie van het incident: de datum en het tijdstip waarop het operationele of beveiligingsincident is geclassificeerd als groot.

Het incident is ontdekt door: geef aan of het incident is ontdekt door een betalingsdienstgebruiker, binnen de betalingsdienstaanbieder (bijv. interne auditfunctie) of door een externe partij (bijv. externe dienstverlener). Geef een toelichting in het daartoe bestemde veld als het geen van de bovengenoemden was.

Soort incident: geef aan of het, voor zover u weet en als de informatie beschikbaar is, om een operationeel of een beveiligingsincident gaat.

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

Beveiliging: niet-geautoriseerde toegang tot of gebruik, openbaarmaking, verstoring, wijziging of vernietiging van de activa van de betalingsdienstaanbieder waardoor de integriteit, beschikbaarheid, vertrouwelijkheid en/of authenticiteit van betalingsgerelateerde diensten wordt beïnvloed. Dit kan zich onder meer voordoen wanneer de betalingsdienstaanbieder een inbreuk op de beveiliging van netwerk- of informatiesystemen ondervindt.

Criteria die aanleiding geven tot melding van groot incident: geef aan welke criteria aanleiding zijn om het grote incident te melden. Er kunnen meerdere criteria worden geselecteerd: getroffen transacties, getroffen betalingsdienstgebruikers, uitvaltijd dienstverlening, inbreuk op de beveiliging van netwerk- of informatiesystemen, economische gevolgen, hoog niveau van interne escalatie, mogelijke gevolgen voor andere betalingsdienstgebruikers of relevante infrastructuren en/of gevolgen voor de reputatie.

Korte, algemene beschrijving van het incident: licht kort de belangrijkste punten van het incident toe, met vermelding van mogelijke oorzaken, onmiddellijke gevolgen, enz.

Impact in andere EU-lidstaten, indien van toepassing: licht kort toe welke impact het incident in andere EU-lidstaten heeft gehad (bijv. op betalingsdienstgebruikers, betalingsdienstaanbieders en/of betalingsinfrastructuren). Geef een vertaling in het Engels, indien dit haalbaar is binnen de termijn voor de melding.

Melding aan andere autoriteiten: geef aan of het incident aan andere autoriteiten is gemeld of zal worden gemeld binnen aparte kaders voor het melden van incidenten, indien bekend ten tijde van de melding. Zo ja, vermeld de respectieve autoriteiten.

Redenen voor late indiening van de initiële melding: geef aan waarom u meer dan 24 uur nodig had om het incident te classificeren.

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 informatie over het specifieke probleem en de achtergrond ervan, hoe het incident is begonnen en zich heeft ontwikkeld, en wat de gevolgen zijn, met name voor betalingsdienstgebruikers, enz. Geef ook informatie over de communicatie met betalingsdienstgebruikers, indien van toepassing.

Hield het incident verband met een of meer eerdere incidenten?: geef aan of er een verband is tussen het incident en eerdere incidenten, indien deze informatie beschikbaar is. Als er een verband is tussen het incident en eerdere incidenten, specificeer dan deze incidenten.

Zijn andere dienstverleners/derde partijen getroffen of bij het incident betrokken?: geef aan of andere dienstverleners/derde partijen door het incident zijn getroffen of erbij betrokken zijn, indien deze informatie beschikbaar is. Als andere dienstverleners/derde partijen door het incident zijn getroffen of erbij betrokken zijn, vermeld deze dan en verstrek nadere informatie.

Is crisismanagement gestart (intern en/of extern)?: geef aan of crisismanagement (intern en/of extern) is gestart. Geef meer informatie, indien crisismanagement is gestart.

Datum en tijdstip van het begin van het incident: de datum en het tijdstip waarop het incident is begonnen, indien bekend.

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.

Getroffen functionele gebieden: geef aan welke stap of stappen van het betaalproces door het incident zijn getroffen, zoals authenticatie/autorisatie, communicatie, clearing, directe afwikkeling, indirecte afwikkeling en anders.

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 over te boeken.

Communicatie: informatiestroom ten behoeve van identificatie, authenticatie, kennisgeving en informatie tussen betalingsdienstaanbieders die de rekeningen beheren 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.

Wijzigingen in eerdere meldingen: geef aan welke wijzigingen zijn aangebracht in de informatie die is verstrekt bij eerdere meldingen met betrekking tot hetzelfde incident (bijv. de initiële of, indien van toepassing, een tussentijdse melding).

B 2 – Classificatie incident/informatie over het incident

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 getroffen transacties ten opzichte van het aantal met dezelfde betalingsdiensten uitgevoerde betalingstransacties dat door het incident is getroffen, en totale waarde van de transacties. Betalingsdienstaanbieders verstrekken concrete waarden voor deze variabelen; dit kunnen werkelijke cijfers of schattingen zijn. 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'. In de gevallen waarin betalingstransacties in andere valuta's dan de euro door het incident zijn getroffen, converteren betalingsdienstaanbieders bij het berekenen van de drempels en het melden van de waarde van de getroffen transacties het bedrag van de transacties in een andere valuta dan de euro naar een bedrag in euro's op basis van de dagelijkse referentiewisselkoers van de ECB voor de dag voorafgaand aan de indiening van de incidentmelding.

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 getroffen betalingsdienstgebruikers ten opzichte van het totale aantal betalingsdienstgebruikers. Betalingsdienstaanbieders verstrekken concrete waarden voor deze variabelen; dit kunnen werkelijke cijfers of schattingen zijn. 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.

Inbreuk op de beveiliging van netwerk- of informatiesystemen: betalingsdienstaanbieders bepalen of een kwaadwillige handeling de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van netwerk- of informatiesystemen (met inbegrip van gegevens) die verband houden met de levering van betalingsdiensten, in gevaar heeft gebracht.

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. Betalingsdienstaanbieders kijken naar 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 waardoor i) het initiëren en/of de uitvoering van een betalingsdienst en/of ii) de toegang tot een betaalrekening onmogelijk is. 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. 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. In de gevallen waarin de kosten zijn gesteld in andere valuta's dan de euro, converteren betalingsdienstaanbieders bij het berekenen van de drempel en bij het melden van de waarde van de economische gevolgen het bedrag van de kosten in een andere valuta dan de euro naar een bedrag in euro's op basis van de dagelijkse referentiewisselkoers van de ECB voor de dag voorafgaand aan de indiening van de incidentmelding.

> **Directe kosten:** kosten (in euro) die het incident direct veroorzaakt, waaronder kosten voor het corrigeren van het incident (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:** kosten (in euro) die het incident indirect veroorzaakt (bijv. schadeloosstellingen/compensaties klanten, mogelijke juridische kosten).

Hoog niveau van interne escalatie: betalingsdienstaanbieders overwegen of, als gevolg van de impact van het incident op betalingsgerelateerde diensten, het leidinggevend orgaan als gedefinieerd door de EBA-richtsnoeren inzake ICT en risicobeheer op het gebied van beveiliging, al of niet, overeenkomstig richtsnoer 60, letter d), van de EBA-richtsnoeren inzake ICT en risicobeheer op het gebied van beveiliging, 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.

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 financiëlemarktinfrastructuren en/of betalingssystemen 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 financiëlemarktinfrastructuren heeft verstoord of waarschijnlijk zal verstoren en of het de solliditeit 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 financiëlemarktinfrastructuren waarvan hij lid is.

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)

betalingsdienstgebruikers en/of andere betalingsdienstaanbieders hebben geklaagd over het nadelige effect van het incident, ii) het incident gevolgen heeft gehad voor een zichtbaar betalingsdienstgerelateerd 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 blogs, sociale netwerken, enz.; aandacht in de media betekent in deze context echter niet alleen een paar negatieve opmerkingen door volgers, maar er moet sprake zijn van een steekhoudend bericht of een significant aantal negatieve opmerkingen/alerts), iii) contractuele verplichtingen niet zijn nagekomen of waarschijnlijk niet zullen worden nagekomen, met als gevolg de publicatie van wettelijke stappen tegen de betalingsdienstaanbieder, iv) wettelijke voorschriften niet zijn nageleefd, met als gevolg de oplegging van toezichtmaatregelen of sancties die openbaar zijn gemaakt of waarschijnlijk openbaar zullen worden gemaakt, en v) of zich eerder een vergelijkbaar incident heeft voorgedaan.

B 3 – Beschrijving incident

Soort incident: operationeel of beveiliging. In het daartoe bestemde veld in de initiële melding wordt een nadere toelichting gegeven.

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 geselecteerd.

In onderzoek: vink dit vakje aan wanneer de oorzaak nog niet bekend is.

Kwaadwillige handeling: handelingen die zich opzettelijk richten tegen de betalingsdienstaanbieder. Hiertoe worden gerekend kwaadaardige code, het vergaren van informatie, inbraken, Distributed/Denial of Service-aanval (D/DoS-aanval), opzettelijke interne handelingen, opzettelijke externe fysieke beschadiging, beveiliging van informatie-inhoud, frauduleuze handelingen en anders. Raadpleeg rubriek C2 van dit formulier voor meer bijzonderheden.

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, netwerken, infrastructuren en databases die de betalingsactiviteit ondersteunen.

Menselijke fouten: 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).

Externe gebeurtenissen: de oorzaak houdt verband met gebeurtenissen die in het algemeen buiten de directe controle van de organisatie liggen (bijv. natuurrampen, een fout van een technische-dienstverlener).

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?: geef aan of het incident rechtstreeks gericht was tegen de betalingsdienstaanbieder of hem indirect treft via een derde partij, indien deze informatie beschikbaar is. Geef in het geval van indirecte impact de naam van de dienstverlener(s).

B 4 – Impact van het incident

Totale impact: geef aan welke aspecten gevolgen hebben ondervonden van het operationele of beveiligingsincident. Er kunnen meerdere antwoorden worden geselecteerd.

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 volledig toegankelijk zijn voor betalingsdienstgebruikers en door hen kunnen worden gebruikt, op vooraf door de betalingsdienstaanbieder vastgelegde, aanvaardbare niveaus.

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.

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.

Elektronische handel (e-handel): de betalingstransactie wordt geïnitieerd op een virtueel verkooppunt (bijv. voor via internet geïnitieerde betalingen waarbij gebruik wordt gemaakt van overboekingen, betaalkaarten, overboeking van elektronisch geld tussen rekeningen voor elektronisch geld).

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 vereist 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.

Overboekingen: 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 incasso's: 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 betalingstransactie 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 betalingstransacties 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 enig 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.

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 het inhield).

C – Eindmelding

C 1 – Algemene informatie

Update van de informatie in de initiële melding en de tussentijdse melding(en) (samenvatting): geef nadere informatie over het incident, met inbegrip van de specifieke wijzigingen die zijn aangebracht in de in de tussentijdse melding verstrekte informatie. Verstrek ook alle overige relevante informatie.

Zijn alle oorspronkelijke controles weer van kracht?: geef aan of de betalingsdienstaanbieder op enig moment tijdens het incident bepaalde controles heeft opgeschort of versoepeld. Zo ja, geef aan of alle controles weer van kracht zijn, en indien dit niet het geval is, geef in het vrijetekstveld aan welke controles nog niet van kracht zijn en hoeveel extra tijd nodig is voor hun herstel.

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, de meest waarschijnlijke oorzaak. Er kunnen meerdere antwoorden worden geselecteerd. (Let op: er moet onderscheid worden gemaakt tussen de onderliggende oorzaak en de impact van het incident.)

Kwaadwillige handeling: externe of interne handelingen die opzettelijk zijn gericht tegen de betalingsdienstaanbieder. Deze zijn onderverdeeld in de volgende categorieën:

Kwaadaardige code: bijv. virus, worm, Trojaans paard, spyware.

Vergaren van informatie: bijv. scannen, snuffelen, social engineering.

Inbraken: bijv. compromitteren van geprivilegieerd account, compromitteren van niet-geprivilegieerd account, compromitteren van applicatie, bot.

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

Opzettelijke interne handelingen: bijv. sabotage, diefstal.

Opzettelijke externe fysieke beschadiging: bijv. sabotage, fysieke aanval op de panden/datacentra.

Beveiliging van informatie-inhoud: niet-geautoriseerde toegang tot informatie, niet-geautoriseerde wijziging van informatie.

Frauduleuze handelingen: niet-geautoriseerd gebruik van middelen, auteursrecht, spoofing, phishing.

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

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). Deze zijn onderverdeeld in de volgende categorieën:

Gebrekkige monitoring en controle: bijv. in verband met werkprocessen, vervaldata van certificaten, vervaldata van licenties, vervaldata van patches, vastgestelde maximale tellerwaarden, vulniveaus van databases, beheer van gebruikersrechten, principe van dubbele controle.

Communicatiekwesties: bijv. tussen marktdeelnemers of binnen de organisatie.

Ongepaste werkzaamheden: bijv. geen uitwisseling van certificaten, cache is vol.

Ontoereikend wijzigingenbeheer: bijv. onbekende configuratiefouten, roll-out met inbegrip van updates, onderhoudskwesties, onverwachte fouten.

Ontoereikendheid van interne procedures en documentatie: bijv. gebrek aan transparantie met betrekking tot functionaliteiten, processen en het optreden van storingen, het ontbreken van documentatie.

Herstelkwesties: bijv. crisisbeheer, ontoereikende redundantie.

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

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, netwerken, infrastructuren en databases die de betalingsactiviteit ondersteunen. Deze zijn onderverdeeld in de volgende categorieën:

Hardwarestoring: storing van fysieke technische apparatuur waarop de processen worden uitgevoerd en/of de gegevens worden opgeslagen die betalingsdienstaanbieders nodig hebben om hun betalingsgerelateerde activiteiten te verrichten (bijv. storing van harde schijven, datacentra, andere infrastructuur).

Netwerkstoring: storing van telecommunicatienetwerken, publiek of privaat, die de uitwisseling van gegevens en informatie (bijv. via internet) tijdens het betaalproces mogelijk maken.

Databaseproblemen: problemen die verband houden met de datastructuur waarin persoonlijke informatie en betalingsgerelateerde informatie wordt opgeslagen die nodig is om betalingstransacties uit te voeren.

Software-/applicatiefout: fouten van programma's, besturingssystemen, enz. die de levering van betalingsdiensten door de betalingsdienstaanbieder ondersteunen (bijv. storingen, onbekende functies).

Fysieke beschadiging: bijv. onbedoelde beschadiging veroorzaakt door gebrekkige omstandigheden, bouwwerkzaamheden.

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

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). Deze fouten zijn onderverdeeld in de volgende categorieën:

Onopzettelijk: bijv. vergissingen, fouten, omissies, gebrek aan ervaring of kennis.

Inactiviteit: bijv. door gebrek aan vaardigheden, kennis, ervaring, bewustzijn.

Onvoldoende middelen: bijv. gebrek aan personele middelen, beschikbaarheid van personeel.

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

Externe gebeurtenis: de oorzaak houdt verband met gebeurtenissen die in het algemeen buiten de controle van de organisatie liggen. Deze zijn onderverdeeld in de volgende categorieën:

Falen van een leverancier/technische-dienstverlener: bijv. stroomuitval, uitval van internet, juridische kwesties, zakelijke kwesties en afhankelijkheden van diensten.

Overmacht: bijv. stroomuitval, brand, natuurlijke oorzaken zoals aardbevingen, overstromingen, zware regenval, harde wind.

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

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

Overige relevante informatie over de onderliggende oorzaak: geef alle aanvullende bijzonderheden over de onderliggende oorzaak, met inbegrip van de voorlopige conclusies die zijn getrokken uit de analyse van de onderliggende oorzaak.

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 wettelijke stappen ondernomen tegen de betalingsdienstaanbieder?: geef aan of er, 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.

Beoordeling van de effectiviteit van de ondernomen stappen: geef, indien beschikbaar, een eigen inschatting van de effectiviteit van de acties die tijdens de duur van het incident zijn ondernomen, met inbegrip van de lessen die uit het incident zijn geleerd.