

Toezicht Nationale  
Instellingen  
Elektronischgeld- &  
Betaalinstellingen

## FAQ's omtrent Fraud Reporting

Op woensdag 25 september 2019 heeft DNB een ronde tafel georganiseerd over de EBA Guidelines on fraud reporting requirements under Directive (EU) 2015/2366. De FAQ's zijn besproken tijdens de fraude ronde tafel en na een consultatieronde uitgewerkt in onderstaand overzicht.

De FAQ's beogen instellingen guidance te bieden bij het invullen en indienen van de fraude rapportages. Indien de EBA en/of ECB via het Q&A proces tot andere antwoorden komt dient DNB deze uit consistentieoverwegingen over te nemen om ervoor te zorgen dat de antwoorden consistent blijven met het Europees regelgevend kader.

**Datum**  
27 februari 2020

**Kenmerk**  
T031-2060830140-29

**Versie**  
2.3

### 1. Definities

#### 1.1 Vraag

**Welke transacties worden er precies bedoeld met 'non-electronic credit transfers'?**

Antwoord:

Non-electronic credit transfers zijn alle transacties die geïnitieerd worden op niet-elektronische basis, waaronder acceptgiro's, OLA/OLO transacties en telefonische transacties.

#### 1.2 Vraag:

**Welke transacties moeten wel/niet gerapporteerd worden onder categorie A Credit Transfers?**

Antwoord:

Enkel uitgevoerde betalingen waar de betaler ('payer') een klant is van de PSP en de betaler de betaling initieert.

#### 1.3 Vraag:

**Hoewel genoemd binnen categorie A Credit transfers, zijn 1.3.2.2.7 en 1.3.2.2.8 niet relevant voor deze categorie?**

Antwoord:

Deze type transacties zijn gespecificeerd in de artikelen 11 en 12 van de RTS on SCA en CSC. De uitzonderingen zijn *channel-agnostic*. Dit houdt in dat hoewel er op dit moment geen businessmodellen zijn die dit type transacties faciliteren, deze niet uitgezonderd worden.

**1.4 Vraag:****Vallen plastic kaarten met token onder categorie C,D,E? Hoe beschouwen we een transfer met NFC, token-based app, smartphone- of watch?**

Antwoord:

Betalingen door middel van tokenized PANs vallen onder de definitie van 'card-based payments'.

**1.5 Vraag****Zijn de transacties die gerapporteerd moeten worden gelimiteerd tot de volgende interpretatie: A 'payment transaction' is the act of transferring funds initiated by a payer or on his behalf, OR an act of withdrawing funds initiated by the payee. Only executed payment transactions and transactions initiated by a payment initiation service provider need to be reported?**

Antwoord:

De definitie van 'payment transaction' betreft een level 1 definitie uit PSD2 (art. 4 lid 5 PSD2) en kan om deze reden in een FAQ niet worden aangepast.

Betaaldienstverleners dienen conform richtsnoer 2.4 enkel uitgevoerde betaaltransacties met inbegrip van geïnitieerde betaaltransacties (betaalinitiatiedienst) te rapporteren. Dit houdt in dat frauduleuze transacties die, voordat zij werden uitgevoerd, zijn tegengehouden wegens een vermoeden van fraude, niet hoeven worden gemeld.

## **2. Rapportage**

### **2.1 Vraag:**

**Moet een frauduleuze transactie van een spaarrekening naar een betaalrekening worden aangemerkt als fraude, ondanks dat er geen geld de rekening verlaat?**

Antwoord:

Rapportage van fraude dient enkel te gebeuren op het moment dat geld een rekening verlaat. In het geval dat er eerst een transactie van spaar naar betaalrekening wordt gemaakt en vervolgens in een nieuwe transactie het geld de betaalrekening verlaat, wordt deze beschouwd als één frauduleuze transactie en dient dus slechts éénmalig gerapporteerd te worden.

### **2.2 Vraag:**

**Moeten transacties van EUR 0,01 gebruikt als rekeningautorisatie worden gerapporteerd als fraude?**

Antwoord:

Deze vorm van transacties laat DNB in principe buiten beschouwing. Als er vervolgttransacties plaatsvinden, dient dit pas gerapporteerd te worden als fraude. Als er volgend op een EUR 0,01 transactie een tweede (grotere) transactie plaatsvindt, kan dit worden beschouwd als een frauduleuze transactie en worden gerapporteerd als één transactie.

### **2.3 Vraag:**

**Wat dient er gerapporteerd te worden in het geval dat de bank geen toegang heeft tot de toestemmingsinformatie?**

Antwoord:

Transacties voor automatische afschrijvingen dienen alleen worden gemeld door de betalingsdianstaanbieder van de begunstigde, aangezien deze transacties worden geïnitieerd door de begunstigde. Zie ook richtsnoer 2.11.

Wanneer een betaaldianstaanbieder voor een bepaalde gegevensuitsplitsing geen gegevens kan rapporteren omdat de desbetreffende gegevensuitsplitsing niet van toepassing is op die betalingsdianstaanbieder, rapporteert hij 'NA' (Not Applicable – niet van toepassing).

## 2.4 Vraag:

**Wat dient er gerapporteerd te worden bij een gestolen of verloren geraakte kaart?**

Antwoord:

Rapporteren dient te gebeuren zoals beschreven in de definitie (C 3.2.2.2.1.1 & C 3.2.2.2.1.2).

## 2.5 Vraag:

**Wat zijn 'executed fraudulent payments'? Welke frauduleuze betalingen moeten wel en welke niet gerapporteerd worden?**

Antwoord:

Betaaldienstverleners rapporteren enkel gegevens over uitgevoerde en geïnitieerde betaaltransacties (overeenkomstig definitie in PSD2). Onder de 'totale frauduleuze betaaltransacties' worden alle transacties gerapporteerd die zijn genoemd in richtsnoer 1.1, ongeacht de vraag of het bedrag van de frauduleuze betaaltransacties is terug verkregen.

## 2.6 Vraag:

**Welke transacties moeten wel/niet gerapporteerd worden onder categorie B Direct Debits?**

Antwoord:

Uitgevoerde betalingen, waarbij de begunstigde een klant is van de PSP en de transactie initieert op basis van de toestemming van de betaler aan de begunstigde.

## 2.7 Vraag:

**Welke transacties moeten wel/niet gerapporteerd worden onder categorie C Cards by Issuer?**

Antwoord:

Betaaldienstverleners verstrekken gegevens voor alle betaaltransacties en frauduleuze betaaltransacties aan de uitgeverszijde (*issuing*) waarbij een betaalkaart is gebruikt en de betaaldienstverlener de betaaldienstaanbieder van de *betaler* was.

## 2.8 Vraag:

### **Welke transacties moeten wel/niet gerapporteerd worden onder categorie D Cards by Acquirer?**

Antwoord:

Betaaldienstaanbieders verstrekken gegevens overeenkomstig gegevensuitsplitsing D voor alle betaaltransacties en frauduleuze transacties aan de accepteerderszijde (*acquiring*) waarbij een betaalkaart is gebruikt en de betaaldienstverlener de betaaldienstaanbieder van de *begunstigde* is.

## 2.9 Vraag:

### **Welke transacties moeten wel/niet gerapporteerd worden onder categorie E Cash Withdrawal?**

Antwoord:

Conform richtsnoer 7.15 dienen betaaldienstverleners gegevens te verstrekken voor alle opnamen van frauduleuze contanten, via apps, bij geldautomaten, bij balies van banken en via detailhandelaars (cashbacks) met gebruikmaking van een kaart.

## 2.10 Vraag:

### **In categorie E is alleen de categorie fraude bij credit card withdrawals uitgewerkt (rijen 5.1 en 5.2). Klopt het zodoende dat er voor debit card withdrawals enkel de totale fraude gerapporteerd moet worden?**

Antwoord:

Betaaldienstverleners dienen de gegevensuitsplitsing aan te houden zoals bedoeld in de Annex van de Guidelines. Vragen met betrekking tot de gegevensuitsplitsing kunnen via de EBA gesteld worden.

### 2.11 Vraag:

#### **Welke transacties moeten wel/niet gerapporteerd worden onder categorie H Payment Initiation?**

Antwoord:

Door PSP geïnitieerde betalingsopdrachten met betrekking tot een rekening bij een andere PSP.

### 2.12 Vraag:

#### **Wat dient er gerapporteerd te worden in het geval van een contactloze low-value betaling bij een unattended terminal for transport or parking fares?**

Antwoord:

Deze zou in de definitie vallen onder beide categorieën. DNB geeft voorkeur aan rapporteren onder de zo specifiek mogelijke categorie. Dit zou in het voorbeeld onder *unattended terminal for transport or parking fares* zijn.

### 2.13 Vraag:

#### **Hoe moeten betaalinstellingen, niet zijnde acquirer, rapporteren voor hun iDEAL transacties? Hoe moeten betaalinstellingen, zijnde acquirer, rapporteren?**

Antwoord:

Om dubbeltellingen te voorkomen dienen betaaldienstverleners van de betaler gegevens in, in haar hoedanigheid van uitgevende of initiërende partij (*issuing*). Indien van toepassing dienen iDEAL transacties gerapporteerd te worden onder Template A, 1.3.1 (of which initiated via remote payment channel) en 1.3.2 (of which initiated via non-remote payment channel).

Een uitzondering hierop vormen gegevens voor kaartbetalingen. Deze worden zowel gemeld door de betaaldienstverlener van de betaler als door de betalingsdienaarbieder van de begunstigde die de betalingstransactie accepteert. De twee perspectieven worden afzonderlijk gemeld, met verschillende uitsplitsingen, zoals aangegeven in bijlage 2.

Betaalinstellingen, zijnde acquirer, dienen frauduleuze transacties te rapporteren voor zover zij daarvan via rapportages van de Card Brands op de hoogte zijn gesteld. Wanneer meer dan één accepterende betalingsdienaarbieder bij een transactie betrokken is, wordt de

rapportage gedaan door de aanbieder die de contractuele relatie heeft met de begunstigde.

#### **2.14 Vraag:**

##### **Waarom moeten credit cards en debit cards geaggregeerd gerapporteerd worden?**

Antwoord:

Het is correct dat deze gezamenlijk gerapporteerd dienen te worden. DNB kan zich vinden in het idee dat dit twee verschillende producten zijn, maar zal de rapportage omwille van Europese consistentie niet aanpassen.

#### **2.15 Vraag:**

##### **Wat wordt de frequentie van het frauderapport?**

Antwoord:

De fraude rapportages zullen voor vergunninghoudende betaaldienstverleners en bijkantoren met zetel in Nederland halfjaarlijks plaatsvinden.

Een uitzondering hierop geldt voor betaaldienstverleners die een vrijstelling hebben op grond van art. 32 van PSD2 en elektronisch geldinstellingen die een ontheffing hebben uit hoofde van art. 9 EMD2. Deze betaaldienstverleners dienen de fraudestatistieken slechts éénmaal per jaar aan te leveren, waarbij de gegevens worden gesplitst in twee periodes van zes maanden.

#### **2.16 Vraag:**

##### **Worden aangepaste versies van de rapportage verwacht door DNB en zo ja hoe vaak?**

Antwoord:

DNB kan, al dan niet op verzoek van ECB/EBA om herrapportage vragen. De frequentie van het opvragen van herrapportages is afhankelijk van de kwaliteit van de aanlevering.

#### **2.17 Vraag:**

##### **Op welke wijze dient de geografische uitsplitsing gerapporteerd te worden?**

In het Digitaal Loket Rapportages is de functionaliteit opgenomen optionele bijlagen toe te voegen. U kunt de geografische splitsing

indienen door separate rapportages conform de gegevensuitsplitsing toe te voegen. Aanvullend dient u in de titel van het bestand de geografische uitsplitsing op te nemen. Ter illustratie:

Rapportagebestanden		Bestand	Extensies	Naam		
Netherlands	➔	XLSX	.xlsx	Data entry template Fraud Repoing_v1.1_Nederland_20191231.xlsx (102.03 KB)	Upload gelukt	✖ Verwijderen <a href="#">Download</a>
Bijlagen <small>OPTIONEEL</small>		Titel	Naam			
Cross-border within the EEA	➔	IX	Data entry template Fraud Repoing_v1.1_crossborderEEA_IX_20191231.xlsx (102.03 KB)			✖ Verwijderen <a href="#">Download</a>
Cross-border outside the EEA	➔	OX	Data entry template Fraud Repoing_v1.1_crossborderNon_EEA_OX_20191231.xlsx (102.03 KB)			✖ Verwijderen <a href="#">Download</a>

Daarnaast dient u in het template in het veld 'GEOGRAPHICAL DIMENSION' tevens deze geografische uitsplitsing te vermelden conform de *naming convention* uitgewerkt in de 'Explanatory Notes' bij het template. Ter illustratie:

	A	B	C	D	E
1	PERIOD	{YYYY}{MM}{DD}	Vul een periode in in de volgende structuur {YYYY}{MM}		
2	VERSION	v1.3			
3	GEOGRAPHICAL DIMENSION		Kies een geografische uitsplitsing: NL, IX of OX		
4					



### **3. Remote vs. Non-remote**

#### **3.1 Vraag:**

**Wat wordt er verstaan onder een 'non-remote payment channel'?**

Antwoord:

Betaaldienstverleners dienen onder de categorie 'non-remote payment channel' betalingstransacties te rapporteren die op een non-remote basis zijn geïnitieerd, bijvoorbeeld POS terminals, ATMs en de fysieke locatie van een bank.

#### **3.2 Vraag:**

**Waar valt een fysieke betaling met 'Pin' of 'Swipe' onder?**

*DNB maakt hier naar aanleiding van de eerste rapportage een nader besluit op.*

### **4. Strong Customer Authentication (SCA)**

#### **4.1 Vraag:**

**Wordt 'verified by visa 2.0' (VBV2.0) gezien als SCA?**

Antwoord:

Een kaartnummer of kaartgegevens worden niet gezien als bewijs van bezit of kennis. Om te worden geaccepteerd als SCA dienen altijd ten minste twee authenticatiemethodes gebruikt te worden, dus dient er in dit geval nog één extra authenticatie te worden toegevoegd. Zie ook de EBA Opinion on the elements of strong customer authentication under PSD2.<sup>1</sup>

#### **4.2 Vraag:**

**Hoe moeten instellingen betaalinstrumenten zonder SCA behandelen?**

Antwoord:

<sup>1</sup> <https://eba.europa.eu/eba-publishes-an-opinion-on-the-elements-of-strong-customer-authentication-under-psd2>

Bij de data breakdown onder 'Of which authenticated via non-strong customer authentication'.

## **5. Modificatie versus manipulatie**

### **5.1 Vraag:**

**Wat verstaat men onder wijziging van een betalingsopdracht door de fraudeur, voorbeelden gewenst.**

Antwoord:

Na het aanhoren van de opinie van de verschillende aanwezige partijen blijkt een verschil te bestaan tussen de definities van manipulatie en modificatie in een aantal specifieke voorbeelden.

Een modificatie van een betalingsopdracht door de fraudeur is een niet-toegestane transactie als gedefinieerd in richtsnoer 1.1, onder a), en betreft een situatie waarin de fraudeur een legitieme betalingsopdracht op enig punt tijdens de elektronische communicatie tussen het apparaat van de betaler en de betalingsdienstaanbieder onderschept en wijzigt (bijvoorbeeld met behulp van malware of een aanval die aanvallers in staat stelt de communicatie tussen twee legitiem communicerende hosts te onderscheppen (man-in-the-middle-aanval) of de betalingsinstructie in het systeem van de betalingsdienstaanbieder wijzigt voordat de betalingsopdracht wordt gecleard en afgewikkeld.

Bij betalingstransacties die zijn verricht doordat de betaler door de fraudeur is gemanipuleerd om te goeder trouw een betalingsopdracht te geven, of de betalingsdienstaanbieder te instrueren dat te doen, naar een betaalrekening waarvan hij gelooft dat deze toebehoort aan een legitieme begunstigde ('manipulatie van de betaler').

### **5.2 Vraag:**

**Wat verstaat men onder manipulatie van de betaler, voorbeelden gewenst?**

Antwoord:

Zie de definitie in richtsnoer 1.1 onder b. Een concreet voorbeeld van manipulatie van de betaler is de zogeheten ceo-fraude. Bij deze vorm van fraude doet de fraudeur zich voor als een reguliere tegenpartij van de betaler en op deze wijze de betaler manipuleert om een betaling te doen naar een betaalrekening waarvan de betaler te goeder trouw gelooft dat deze tot een rechtmatige begunstigde behoort.

### 5.3 Vraag:

**Welke frauduleuze transacties moeten wel/niet onder 'modification by fraudster' worden verstaan?**

Antwoord:

Wijziging van een betalingsopdracht door de fraudeur is een vorm van een niet-toegestane transactie, waarbij de fraudeur a) een rechtmatige betalingsopdracht wijzigt op een bepaald moment tijdens de elektronische communicatie tussen het apparaat van de betaler en de betalingsdienstaanbieder of; b) de betalingsinstructie in het systeem van de betalingsdienstaanbieder wijzigt voordat de betalingsopdracht wordt goedgekeurd en afgewikkeld (voorbeelden zijn malware of een man-in-the-middle-aanval).

### 5.4 Vraag:

**Welke frauduleuze transacties moeten onder de MO 'manipulation of the payer' worden verstaan?**

Antwoord:

Dit houdt in dat de betaler wordt gemanipuleerd door de fraudeur om een betalingsopdracht te geven, of om de opdracht daartoe te geven aan de betalingsdienstaanbieder, te goeder trouw, op een betaalrekening die volgens hem toebehoort aan een rechtmatige begunstigde. Een overval of fysieke bedreiging om een geldopname of kaarttransactie uit te voeren is geen manipulatie te goeder trouw.

### 5.5 Vraag:

**Moeten CPSP's in het geval van fraude met cadeaukaarten rapporteren?**

Antwoord:

Het antwoord op deze vraag is sterk afhankelijk van de functies die de e-money card biedt. Op basis van de definitie moet dit omdat het op kaarten gebaseerde transacties zijn en er dus van twee kanten gerapporteerd kan worden. Aan de andere kant wordt in de bijlage (D) een kaart met alleen een elektronisch geldfunctie uitgezonderd van de op kaarten gebaseerde betalingstransacties.

Zie ook richtsnoer 1.5 waarin wordt vermeld dat indien er sprake is van verschillende betalingsdienstaanbieders, de betaling alleen wordt gemeld door de betalingsdienstaanbieder van de betaler, om dubbelbetalingen te voorkomen.