DeNederlandscheBank
EUROSYSTEEM

**FAQs on fraud reporting**

Toezicht Nationale Instellingen Elektronischgeld- & Betaalinstellingen

We hosted a roundtable session on the EBA Guidelines on fraud reporting under the Payment Services

Directive 2 (PSD2) on 25 September 2019. We discussed frequently asked questions and decided to list them in this document, following a round of consultations.

These FAQs should offer financial institutions guidance when completing and submitting fraud reports. If the EBA's or ECB's answers to Q&As differ from our answers, we will adopt their answers, as answers to Q&As must be consistent with the European regulatory framework.

**Datum**
27 February 2020

**Kenmerk**
T031-2060830140-29

**Version**
2.3

## 1. Definitions

### 1.1 Question

**What exactly are "credit transfers initiated non-electronically"?**

Answer:

This transaction type includes giro collection forms and optically readable giro collection and credit transfer forms, as well as telephone transactions.

### 1.2 Question:

**Which transactions must and must not be reported under category A "credit transfers"?**

Answer:

Only those in which the payer is a customer of the payment service provider and initiates the payment.

### 1.3 Question:

**Although transaction types 1.3.2.2.7 and 1.3.2.2.8 are listed under category A "credit transfers", are they not relevant?**

Answer:

These transaction types are specified in Articles 11 and 12 of the regulatory technical standards (RTS) on strong customer authentication (SCA) and common and secure communication (CSC). The exceptions are channel-agnostic, which means that they are not excepted, although

there are currently no business models that support these transaction types.

### 1.4 Question:

**Do plastic cards with a token fall under categories C, D and E? How should we treat credit transfers made with NFC, a token-based app, a smartphone or a smartwatch?**

Answer:

Payments using a tokenised primary account number (PAN) come under the definition of card-based payments.

### 1.5 Question

**Are transactions that must be reported limited to the following definition: "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"?**

Answer:

This is a level 1 definition of "payment transaction", given in Article 4(5) of PSD2, so we cannot modify it for the purposes of these FAQs.

Guideline 2.4 provides that payment service providers must report only payment transactions that have been executed, including those transactions that have been initiated (payment initiation service). This means that suspicious transactions that were blocked before they were executed due to suspicion of fraud do not need to be included.

## 2. Reporting

### 2.1 Question:

**Must a suspicious transaction from a savings accounts to a payment account be considered fraudulent even if no funds leave the account?**

Answer:

Fraud must be reported only after funds have left an account. If, in the first transaction, funds are first transferred from a savings account to a payment account and subsequently, in the second transaction, they

leave the payment account, they are considered a single fraudulent transaction. Accordingly, they must be reported once.

### 2.2 Question:

**Must EUR 0.01 transactions that are used as account authorisation be reported as fraudulent?**

Answer:

As a rule, we do not deal with this type of transactions. Only subsequent transactions must be reported as fraudulent. If a second, larger, transaction follows the EUR 0.01 transaction, it can be considered fraudulent and reported as a single transaction.

### 2.3 Question:

**What must be reported if the bank has no access to the consent information?**

Answer:

For direct debits, transactions must be reported by the payee's payment service provider only, given that these transactions are initiated by the payee. See also Guideline 2.11.

If a payment service provider cannot report data for a specific breakdown because that particular data breakdown is not applicable to that PSP, the data must be reported as "NA" for not applicable.

### 2.4 Question:

**What must be reported if a card is stolen or lost?**

Answer:

This must be reported in accordance with the definition (C 3.2.2.2.1.1 and C 3.2.2.2.1.2).

### 2.5 Question:

**What are "executed fraudulent payments"? Which fraudulent payments must and must not be reported?**

Answer:

Payment service providers must only report data on executed and initiated payment transactions, in accordance with the definition given in

PSD2. Under "total fraudulent payment transactions", all transactions referred to in Guideline 1.1 must be reported, regardless of whether the amount of the fraudulent transactions was retrieved.

### 2.6 Question:

**Which transactions must and must not be reported under category B "direct debits"?**

Answer:

Executed payments in which the payee is a customer of the payment service provider and initiates the payment based on the payer's consent given to the payee.

### 2.7 Question:

**Which transactions must and must not be reported under category C "card-based payment transactions to be reported by the issuing payment service provider"?**

Answer:

Payment service providers must provide data for all payment transactions and fraudulent payment transactions on the issuer's side if a payment card was used and the payment service provider was the *payer's* payment service provider.

### 2.8 Question:

**Which transactions must and must not be reported under category D "card-based payments transactions to be reported by the acquiring payment service provider"?**

Answer:

Payment service providers must provide data in accordance with Data Breakdown D for all payment transactions and fraudulent payment transactions on the acquiring side if a payment card was used and the payment service provider is the *payee's* payment service provider.

**2.9 Question:**

**Which transactions must and must not be reported under category E "cash withdrawals"?**

Answer:

In conformity with Guideline 7.15, payment service providers must provide data for all fraudulent cash withdrawals through apps, at ATMs, at bank counters and through retailers ("cash back") using a card.

**2.10 Question:**

**Category E only breaks down fraudulent cash withdrawals with a credit card (rows 5.1 to 5.2). Does this mean that fraudulent cash withdrawals with a debit card must only be reported as an aggregate?**

Answer:

Payment service providers must apply the data breakdown as set out in the Annex to the Guidelines. Any questions about data breakdown can be directed to the EBA.

**2.11 Question:**

**Which transactions must and must not be reported under category H "transactions initiated by payment initiation service providers"?**

Answer:

Payment orders initiated by a payment service provider relating to an account held at another payment service provider.

**2.12 Question:**

**What must be reported in the event of a contactless low-value payment at an unattended terminal for transport or parking fares?**

Answer:

Under the definition, this would fall under both categories, i.e. both 1.3.2.2.7 and 1.3.2.2.8. We prefer reporting under the most specific category, meaning "unattended terminal for transport or parking fares" in this specific example.

**2.13 Question:**

**How must non-acquiring payment institutions report their iDEAL transactions? How must acquiring payment institutions report their transactions?**

Answer:

To avoid double counting, a payer's payment service provider must report data in the capacity of issuing payment institution. Where applicable, iDEAL transactions must be reported under Template A, 1.3.1 ("of which initiated via remote payment channel") and 1.3.2 ("of which initiated via non-remote payment channel").

The only exceptions to this are data for card payments, which are reported by both the payer's and the payee's payment service provider. These two perspectives are reported separately, with different data breakdowns in accordance with Annex 2.

Acquiring payment institutions must report fraudulent transactions if they were informed of them in reports from the card brands. If more than one acquiring payment provider is involved in a transaction, the provider that has a contractual relationship with the payee must report the data.

**2.14 Question:**

**Why must fraudulent transactions with debit and credit cards be reported as an aggregate?**

Answer:

These two types of transactions must be reported as a combined report although we believe they are two distinct product types. We will not make any changes, however, to maintain consistent reporting throughout Europe.

**2.15 Question:**

**What will be the reporting frequency for fraud reporting?**

Answer:

The reporting frequency for licensed payment service providers with registered office or branch offices in the Netherlands will be every six months.

An exception applies to payment service providers that are exempted under Article 32 of PSD2 and electronic money institutions that are exempted under Article 9 of the Second E-money Directive (EMD2). The reporting frequency for these institutions is once a year, with the data

broken down into two six-month periods.

### 2.16 Question:

**Does DNB expect to request adjustments to reports and, if so, how often?**

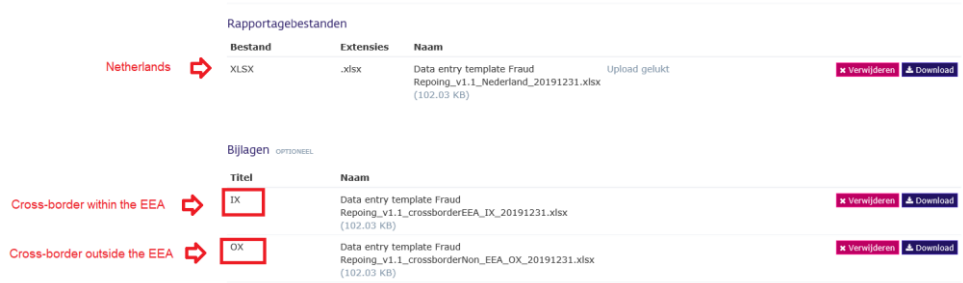
Answer:

We may ask institutions to make resubmissions, also at the request of the ECB or EBA. Their frequency will depend on the quality of the reports.

### 2.17 Question:

**How must the geographical breakdown be reported?**

Our Digital Reporting Portal (*Digitaal Loket Rapportages*) has the option of attaching non-mandatory files. You can submit the geographical breakdown by adding separate reports in accordance with the data breakdown. In addition, you must include the geographical breakdown in the title of the attached file. For illustration:




In addition, you also need to state this geographical breakdown in the template in the field "GEOGRAPHICAL DIMENSION" in accordance with the naming convention detailed in the "Explanotary Notes" with the template. As an example:

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

## 3. Remote or non-remote

### 3.1 Question:

**What exactly is a "non-remote payment channel"?**

Answer:

Payment service providers must report payment transactions under the "non-remote payment channel" category if they were initiated on a non-remote basis, for example using a POS terminal, an ATM or a physical bank branch.

### 3.2 Question:

**How must fraudulent physical payment transactions using PIN or swipe be reported?**

*We will decide on this after we have assessed the first reports.*

## 4. Strong Customer Authentication (SCA)

### 4.1 Question:

**Is "verified by visa 2.0" (VBV2.0) considered a type of SCA?**

Answer:

A card number or card data are not considered evidence of possession or knowledge. Acceptance as SCA requires at least two authentication methods, meaning that at least one method must be added. See also EBA Opinion on the elements of strong customer authentication under PSD2.[1]

### *4.2* Question:

**How must payment institutions report payment instruments without SCA?**

Answer:

Payment institutions must report these under the category "of which authenticated via non-strong customer authentication".

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

## 5. Modification or manipulation

### 5.1 Question:

**What exactly is modification of a payment order by the fraudster? Please provide examples.**

Answer:

After various attendants of the roundtable session had given their opinion, a discrepancy appeared between the definitions of manipulation and modification in several specific examples.

Modification of a payment order by the fraudster is a type of unauthorised transaction as defined in Guideline 1.1(a) and refers to a situation where the fraudster intercepts and modifies a legitimate payment order at some point during the electronic communication between the payer's device and the payment service provider (for instance through malware or attacks allowing attackers to eavesdrop on the communication between two legitimately communicating hosts (man-in-the middle attacks)) or modifies the payment instruction in the payment service provider's system before the payment order is cleared and settled.

Payment transactions made as a result of the payer being manipulated by the fraudster to issue a payment order, or to give the instruction to do so to the payment service provider, in good-faith, to a payment account it believes belongs to a legitimate payee ("manipulation of the payer").

### 5.2 Question:

**What exactly is manipulation of the payer by the fraudster to issue a payment order? Please provide examples.**

Answer:

See the definition in Guideline 1.1(b). CEO fraud is a specific example of manipulation of the payer. In this type of fraud, the fraudster poses as one of the payer's regular counterparties, manipulating the payer into making a payment to a payment account it believes, in good faith, belongs to a legitimate payee.

### 5.3 Question:

**Which fraudulent transactions must or must not be considered "modification by fraudster"?**

Answer:

Modification of a payment order by the fraudster is a type of unauthorised transaction and refers to a situation where the fraudster a) intercepts and modifies a legitimate payment order at some point during the electronic communication between the payer's device and the payment service provider, or b) modifies the payment instruction in the payment service provider's system before the payment order is cleared and settled (for instance through malware or man-in-the middle attacks).

### 5.4 Question:

**Which fraudulent transactions must be considered "manipulation of the payer"?**

Answer:

This involves the payer being manipulated by the fraudster to issue a payment order, or to give the instruction to do so to the payment service provider, in good-faith, to a payment account it believes belongs to a legitimate payee. Robbery or physical threat to coerce someone into making a cash withdrawal or perform a card transaction does not qualify as manipulation to issue a payment order in good faith.

### 5.5 Question:

**Must collecting payment service providers submit a report in the event of fraud involving gift cards?**

Answer:

This depends greatly on the functions which the e-money card offers. Based on the definition, fraud must be reported as it involves a card-based payment transaction, meaning it can be reported from both sides. However, Section D of Annex 2 exempts cards with an e-money function only from card-based payment transactions.

See also Guideline 1.5, which states that if the payment service providers are different, payment is only reported by the payer's payment service provider to avoid double counting.