FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Fraud reporting to Finanstilsynet

Guidelines

DATE:
01.07.2023

NUMBER:
Version 1.2

THE GUIDE APPLIES TO:
BANKS, CREDIT INSTITUTIONS, E-MONEY INSTITUTIONS, PAYMENT INSTITUTIONS AND SUBSIDIARIES OF SUCH INSTITUTIONS OPERATING IN NORWAY

Contents

1 Introduction

In accordance with Article 96(6) of Directive (EU) 2015/2366 (PSD 2) shall payment service providers (PSP) provide, at least on an annual basis, statistical data on fraud relating to different means of payment to their competent authorities, and competent authorities shall provide aggregate data to the European Banking Authority (EBA) and the European Central Bank (ECB).

PSD 2 Article 96(6) is incorporated in the Regulations on Payment Services Systems Section 2, sub-section 4, where it states that: "Payment service providers shall report statistics on fraud related to payment services to Finanstilsynet at least annually, as Finanstilsynet states."

In this guide Finanstilsynet advises on how to conduct the fraud reporting.

EBA has in cooperation with ECB set out guidelines[1] that provide detail on statistical data on fraud related to different means of payment that payment service providers (PSPs) have to report to their competent authorities, as well as on the aggregated data that the competent authorities have to share with the EBA and the ECB, in accordance with Article 96(6).

The guidelines were amended with effect for the reporting from the second half of 2020. This guide describes how the PSPs are to carry out the fraud reporting in accordance with the amended guidelines from the EBA.

The reporting obligation does not apply to account information service providers.

Starting with the reporting for H1 2023, Finanstilsynet also asks for a simplified reporting of prevented fraud.

1.1 Reporting period and first reporting

Finanstilsynet has decided that the institutions shall report fraud statistics to Finanstilsynet semi-annually. This is a continuation of previous practice of semi-annually fraud reporting to Bits AS, the financial infrastructure company of the bank and finance industry in Norway, and is in line with EBA's guidelines.

For PSPs who operate through their head office in Norway or branch in Norway, the first reporting period is the second half of 2019 with deadline for the first reporting on 15 March 2020.

[1] https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-fraud-reporting-under-psd2

2 Reporting format

The data shall be reported in an Excel form developed by Finanstilsynet in accordance with the specifications in the EBA guidelines. When submitting the data to Finanstilsynet, the institution must use the Altinn portal and form no. KRT-1132, with the Excel form attached.

In the KRT-1132 form the institution shall inform about reporting PSP, reporting year, reporting period (first or second half year), and whether there are initial data for the period or revised data for the period.

The Excel form consists of a cover page, one sheet for each of the types of payment transactions and a sheet with validation rules.

The types of payment transactions to be reported are:

- credit transfers
- direct debits
- card-based payment transactions to be reported by the issuer's payment service provider
- card-based payments transactions to be reported by the acquirer's payment service provider
- cash withdrawals using cards
- e-money payment transactions
- money remittance payment transactions
- transactions initiated by payment initiation service providers (PIS transactions)

The field codes in the left column of the payment transactions sheets refer to the field codes in the corresponding tables in Annex 2 of the EBA guidelines.

3 Reporting instructions for the Excel form

3.1 Details of filling in the fields

The institutions must report the total volume of payment transactions (the number of transactions) and the total value of the payment transactions (the sum of the value of the transactions) and the volume (number) of the fraudulent transactions and the value (the sum of the value) of the fraudulent transactions during the reporting period.

Volume shall be reported without decimals.
Value shall be reported in Norwegian kroner (NOK). Value shall be reported by using two decimal places.

Note: From the reporting for the second half of 2020, the value must be reported in NOK, not in full NOK 1000 as before.

The reporting distinguishes between domestic payments, cross-border transactions to

countries within the EEA and cross-border transactions to countries outside the EEA.

3.2 Payer PSP versus payee PSP

In line with the EBA guideline all payment transactions shall be reported from the payer's PSP perspective, except for direct debit transactions where reporting is from the payee's PSP perspective and card-based payment transactions where separate reporting is envisaged from both the issuer's and the acquirer's PSP perspective.

3.3 Losses due to fraud per liability bearer

Except for the money remittance transactions and transactions initiated by payment initiation services providers, *'losses due to fraud per liability bearer*' shall be reported.
It shall be reported:

- who is carrying the loss as a result of the fraud
- the value of the loss in NOK

There are three field codes per type of payment transaction, all starting with the number '9', and containing the indication of the liability bearer:

- 'PSP' means the reporting payment service provider.
- 'PSU' means the payment service user.
- 'O' means others.

3.4 Data validation

The cells in the Excel form with pre-filled data, formulas or specific data validation are protected to ensure the quality and consistency of the data being reported. Areas not to be filled in are blocked.

Validation and summation rules have been included in the Excel sheets in accordance with what is specified in 'Annex 2 – Data reporting requirements for payment service providers' in the EBA guidelines. The validation rules are added to the Excel form in a separate sheet.

The validation rules shall, among other things, ensure that both volume and value are filled in, and that the volume and value for fraudulent transactions are lower than for corresponding total transactions.

For some fields, there are summation rules over two dimensions of the data, both of which should give the same answer. This is identified in the validation rules by two rules giving the same answer.

Example:

Sheet 'Card payments – issuer' – row 8, **'3.2.1 Of which initiated via remote payment channel'**.

Here, both

the sum of 3.2.1.1.1 and 3.2.1.1.2 (debit cards and credit cards) and
the sum of 3.2.1.2 and 3.2.1.3 (with and without strong customer authentication)

shall be equal to **3.2.1**.

The values in row 8 for 3.2.1 will be red until both conditions are met.

If a field is red, there are checks that are not met. The defect must be identified, and it must be filled in again. No fields should be red when submitting the form.

3.5 Card-based and e-money transactions without strong customer authentication (SCA)

Reporting cross-border transactions without SCA to countries outside the EEA can create problems if the non-EEA party, whether issuing or redeeming, does not support SCA and is not subject to PSD 2 requirements. In such cases, one will not find the reason for non-strong customer authentication among those alternatives it is possible to report on in the form. The same can also apply to some other types of payments.

The problem concerns card-based transactions and e-money transactions where e-money is stored on prepaid cards. This could affect the validation formulas in the Excel sheets in question, so that the sum of the '*... different reasons for authentication without strong customer authentication*' does not necessarily match the aggregated indicator '*... of which authenticated without strong customer authentication*'.

To solve this, a row is added at the relevant locations in the Excel sheets, with the text '*Other reasons for non-strong customer authentication*'. There you may fill in the transactions for which you cannot specify why SCA is not being used.

Note: The rows '*of which initiated without strong customer authentication*' are examples of fields where there are summation rules across two dimensions of the data, both of which should give the same answer.

Example:

Sheet 'Card payments – issuer' – row 22, **'3.2.1.3 Of which Authenticated via non-strong customer authentication'**

For fraudulent transactions, both
the sum of 3.2.1.3.1 and 3.2.1.3.2 and 3.2.1.3.3 (different types of scams) and
the sum of 3.2.1.3.4 - 3.2.1.3.10 (reasons for lack of strong customer authentication)

shall be equal to **3.2.1.3**.

The values in row 22 for 3.2.1.3 will be red until both conditions are met.

3.6 Cash withdrawals

As noted, the field codes in the left column of the Excel sheets refer to the field codes in the corresponding tables in Annex 2 of the EBA guidelines.

In the EBA's amended guidelines, the table for Cash Withdrawals in Annex 2 has been changed so that it corresponds to the use of numbering under 5.3 for '*of which different types of card payment fraud*' in the Excel sheet for cash withdrawals. The breakdown into types of payment fraud must cover fraud both with debit cards and with credit cards and sort directly under 5.

This is another example where there are summation rules across two dimensions of the data, both of which should give the same answer:

Sheet 'Cash withdrawals' – row 5, **'5 Cash withdrawals'**:

For fraudulent transactions both
the sum of 5.1 and 5.2 (debit cards and credit cards) and
the sum of 5.3.1 and 5.3.2 (types of fraudulent payments)

shall be equal to **'5 Cash withdrawals'**.

The values in row 5 for 5 will be red until both conditions are met.

3.7 Revised data

If there is a need to adjust data for a specified reporting period, the adjustments should be reported within the subsequent reporting period after the institution has obtained updated/corrected information.

The institutions must send revision of previously submitted data as a separate submission with a similar Excel form as the original submission.

The submittance of revised data must include **all** data, not only revised data.

The deadline for submitting revised data for the previous reporting period is the same as the deadline for the ordinary data submission.

3.8 Prevented fraud

Finanstilsynet is aware that payment service providers prevent a large number of fraudulent transactions, making the potential losses greater than the reported losses. To get a clearer picture of the current threat landscape and the scope of fraudulent activity, Finanstilsynet requests a simplified reporting of prevented fraudulent transactions. Prevented fraudulent transactions include all transactions that have been initiated through fraudulent activity, but have been stopped either manually, through transaction monitoring systems, or in other ways.

The reporting of prevented fraudulent activity is limited to PSPs that provide payment services reported as "Credit transfers" and/or "Cards (issuer)". The reported data should not separate between domestic transactions, cross-border within the EEA, or cross-border outside the EEA, but should rather be reported altogether in a *combined* number.

The reporting of fraudulent transactions applies from the beginning of H1 2023 and is to be made in a new worksheet called "Prevented fraud" in the Excel form KRT-1132. Four numbers are to be reported:

- Credit transfers: The number of prevented transactions and the total value in NOK
- Card transactions: The number of prevented transactions and the total value in NOK

FINANSTILSYNET
P.O.Box 1187 Sentrum
NO-0107 Oslo
POST@FINANSTILSYNET.NO
WWW.FINANSTILSYNET.NO