Guidelines

on reporting requirements for fraud data under Article 96(6) PSD2

Version updated on 20/12/2018 to reflect editorial changes applied to pages 4, 27, 29 and 30

1. Compliance and reporting obligations

Status of these Guidelines

1. This document contains Guidelines issued pursuant to Article 16 of Regulation (EU) No 1093/2010[1]. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities and financial institutions must make every effort to comply with the Guidelines.

2. Guidelines set out the EBA's view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authorities as defined in Article 4(2) of Regulation (EU) No 1093/2010 to whom Guidelines apply should comply by incorporating them into their practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where Guidelines are directed primarily at institutions.

Reporting requirements

3. According to Article 16(3) of Regulation (EU) No 1093/2010, competent authorities must notify the EBA that they comply or intend to comply with these Guidelines or otherwise give reasons for non-compliance, by ([dd.mm.yyyy]). In the absence of any notification by this deadline, competent authorities will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form available on the EBA website to compliance@eba.europa.eu with the reference 'EBA/GL/2018/xx'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities. Any change in the status of compliance must also be reported to the EBA.

4. Notifications will be published on the EBA website, in line with Article 16(3).

[1] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC, (OJ L 331, 15.12.2010, p.12).

2. Subject matter, scope and definitions

Subject matter

5. These Guidelines provide detail on statistical data on fraud related to different means of payment that payment service providers 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) of Directive (EU) 2015/2366 (PSD2).

Scope of application

6. These Guidelines apply in relation to the reporting by payment service providers to competent authorities of statistical data on fraud for payment transactions that have been initiated and executed (including acquired where applicable), including the acquiring of payment transactions for card payments, identified by reference to: (a) fraudulent payment transactions data over a defined period of time and (b) payment transactions over the same defined period.

7. Data reported under the credit transfers breakdown should include credit transfers performed via automated teller machines with a credit transfer function. Credit transfers used to settle outstanding balances of transactions using cards with a credit or delayed debit function should also be included.

8. Data reported under the direct debit breakdown should include direct debits used to settle outstanding balances of transactions using cards with a credit or delayed debit function.

9. Data reported under the card payments breakdowns should include data on all payment transactions by means of payment cards (electronic and non-electronic). Payments with cards with an e-money function only (e.g. prepaid cards) should not be included in card payments but be reported as e-money.

10. These Guidelines also set out how competent authorities should aggregate the data mentioned in paragraph 6 that shall be provided to the ECB and the EBA in accordance with Article 96(6) PSD2.

11. The Guidelines are subject to the principle of proportionality, which means that all payment service providers within the scope of the Guidelines are required to be compliant with each Guideline, but the precise requirements, including on frequency of reporting, may differ between payment service providers, depending on the payment instrument used, the type of services provided or the size of the payment service provider.

Addressees

12. These Guidelines are addressed to:

- payment service providers as defined in Article 4(11) of Directive (EU) 2015/2366 (PSD2) and as referred to in the definition of 'financial institutions' in Article 4(1) of Regulation (EU) No 1093/2010, except account information service providers, and to

- competent authorities as defined in point (i) of Article 4(2) of Regulation (EU) No 1093/2010.

Definitions

13. Unless otherwise specified, terms used and defined in Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions, in Regulation (EU) No 260/2012 of the European Parliament and of the Council establishing technical and business requirements for credit transfers and direct debit in euro, in Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market and in Directive 2009/110/EC of the European Parliament and of the Council on the taking up, pursuit and prudential supervision of the business of electronic money institutions have the same meaning in these Guidelines.

Date of application

14. These Guidelines apply from 1 January 2019, with the exception of the reporting of data related to the exemptions to the requirement to use strong customer authentication provided for in Commission Delegated Regulation (EU) 2018/389 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, which will be applicable from 14 September 2019. The data relating to these exemptions are detailed in Annex 2 in Data Breakdowns A (*1.3.1.2.4 to 1.3.1.2.9 and 1.3.2.2.4 to 1.3.2.2.8*), C (*3.2.1.3.4 to 3.2.1.3.8 and 3.2.2.3.4 to 3.2.2.3.7*), D (*4.2.1.3.4 to 4.2.1.3.6 and 4.2.2.3.4 to 4.2.2.3.6*) and F (*6.1.2.4 to 6.1.2.9 and 6.2.2.4 to 6.2.2.7*).

3.1 Guidelines on fraud data reporting applicable to Payment Service Providers

Guideline 1: Payment transactions and fraudulent payment transactions

1.1. For the purposes of reporting statistical data on fraud in accordance with these Guidelines, the payment service provider should report for each reporting period:

a. unauthorised payment transactions made, including as a result of the loss, theft or misappropriation of sensitive payment data or a payment instrument, whether detectable or not to the payer prior to a payment and whether or not caused by gross negligence of the payer or executed in the absence of consent by the payer ('unauthorised payment transactions'); and

b. 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').

1.2. For the purposes of Guideline 1.1, the payment service provider (including the payment instrument issuer where applicable) should report only payment transactions that have been initiated and executed (including acquired where applicable). The payment service provider should not report data on payment transactions that, however linked to any of the circumstances referred to in Guideline 1.1, have not been executed and have not resulted in a transfer of funds in accordance with PSD2 provisions.

1.3. In the case of money remittance services where funds were transferred from a payer's payment service provider to a payer's money remitter payment service provider (as part of a money remittance payment transaction), it is the payer's payment service provider, rather than the money remitter payment service provider, who should report the payment transactions from the payer's payment service provider to the money remitter. Such transactions should not be reported by the payment service provider of the beneficiary of the money remittance payment transaction.

1.4. Transactions and fraudulent transactions where funds have been transferred by a money remitter payment service provider from its accounts to a beneficiary account, including through arrangements offsetting the value of multiple transactions (netting arrangements), should be reported by the money remitter payment service provider in accordance with Data Breakdown G in Annex 2.

1.5. Transactions and fraudulent transactions where e-money has been transferred by an e-money provider to a beneficiary account, including where the payer's payment service provider is identical to the payee's payment service provider, should be reported by the e-money provider in accordance with Data Breakdown F in Annex 2. Where the payment service providers are different, payment is only reported by the payer's payment service provider to avoid double counting.

1.6. Payment service providers should report all payment transactions and fraudulent payment transactions in accordance with the following:

a. 'Total fraudulent payment transactions' refer to all transactions mentioned in Guideline 1.1, regardless of whether the amount of the fraudulent payment transaction has been recovered.

b. 'Losses due to fraud per liability bearer' refers to the losses by the reporting payment service provider, its payment service user or others, reflecting the actual impact of fraud on a cash flow basis. Since the registering of financial losses borne may be disassociated time-wise from the actual fraudulent transactions and in order to avoid revisions of reported data purely due to this immanent time lag, the final fraud losses should be reported in the period when they are recorded in the payment service provider's books. The final fraud loss figures should not take into account refunds by insurance agencies because they are not related to fraud prevention for the purposes of PSD2.

c. '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.

d. 'Issuance 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 a fake payment order is issued by the fraudster after having obtained the payer/payee's sensitive payment data through fraudulent means.

Guideline 2: General data requirements

2.1. The payment service provider should report statistical information on:

a. total payment transactions in line with the different breakdowns in Annex 2 and in accordance with Guideline 1; and

b. total fraudulent payment transactions in line with the different breakdowns in Annex 2 and as defined in Guideline 1.6(a).

2.2. The payment service provider should report the statistical information specified in Guideline 2.1 in terms of both volume (i.e. number of transactions or fraudulent transactions) and value (i.e. amount of transactions or fraudulent transactions). They should report volumes and values in actual units, with two decimals for values.

2.3. A payment service provider authorised, or a branch established, in a Member State of the euro area should report the values in euro currency, whereas a payment service provider authorised, or a branch established, in a Member State not participating in the euro area should report in the currency of that Member State. The reporting payment service providers should convert data for values of transactions or fraudulent transactions denominated in a currency other than the euro currency or the relevant Member State's official currency into the currency they should report in, using the relevant exchange rates applied to these transactions or the average ECB reference exchange rate for the applicable reporting period.

2.4. The payment service provider should report only payment transactions that have been executed, including those transactions that have been initiated by a payment initiation service provider. Prevented fraudulent transactions that are blocked before they are executed due to suspicion of fraud should not be included.

2.5. The payment service provider should report the statistical information with a breakdown in accordance with the breakdowns specified in Guideline 7 and compiled in Annex 2.

2.6. The payment service provider should identify the applicable data breakdown(s), depending on the payment service(s) and payment instrument(s) provided, and submit the applicable data to the competent authority.

2.7. The payment service provider should ensure that all data reported to the competent authority can be cross-referenced in accordance with Annex 2.

2.8. The payment service provider should allocate each transaction to only one sub-category for each row of each data breakdown.

2.9. In the case of a series of payment transactions being executed, or fraudulent payment transactions being executed, the payment service provider should consider each payment transaction or fraudulent payment transaction in the series to count as one.

2.10. The payment service provider can report zero ('0') where there were no transactions or fraudulent transactions taking place for a particular indicator in the reporting period established. Where the payment service provider cannot report data for a specific breakdown because that particular data breakdown is not applicable to that PSP, the data should be reported as 'NA'.

2.11. For the purpose of avoiding double-counting, the payer's payment service provider should submit data in its issuing (or initiating) capacity. As an exception, data for card payments should be reported both by the payer's payment service provider and by the payee's payment service provider acquiring the payment transaction. The two perspectives should be reported separately, with different breakdowns as detailed in Annex 2. In the event that there is more than one acquiring payment service provider involved, the provider that has the contractual relationship with the payee should report. In addition, for direct debits, transactions must be reported by the payee's payment service provider only, given that these transactions are initiated by the payee.

2.12. In order to avoid double counting when calculating the total transactions and fraudulent transactions across all payment instruments, the payment service provider that executes credit transfers initiated by a payment initiation service provider should indicate the breakdown for the volume and value of the total transactions and fraudulent payment transactions that have been initiated via a payment initiation service provider when reporting under Data Breakdown A.

Guideline 3: Frequency, reporting timelines and reporting period

3.1. The payment service provider should report data every six months based on the applicable data breakdown(s) in Annex 2.

3.2. The payment service provider that benefit from an exemption under Article 32 PSD2 and e-money institutions that benefit from the exemption under Article 9 Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions should only report the set of data requested under the applicable form(s) in Annex 2 on an annual basis with data broken down in two periods of six months.

3.3. The payment service provider should submit their data within the timelines set by the respective competent authorities.

Guideline 4: Geographical breakdown

4.1 The payment service provider should report data for transactions that are domestic, cross border within the European Economic Area (EEA), and cross-border outside the EEA.

4.2 For non-card based payment transactions, and remote card based payment transactions, 'domestic payment transactions' refer to payment transactions initiated by a payer, or by or through a payee, where the payer's payment service provider and the payee's payment service provider are located in the same Member State.

4.3 For non-remote card-based payment transactions, 'domestic payment transactions' refer to payment transactions where the payer's payment service provider (issuer), the payee's payment service provider (acquirer) and the point of sale (POS) or automated teller machine (ATM) used are located in the same Member State.

4.4 For EEA branches, domestic payment transactions refer to the payment transactions where both the payer's and the payee's payment service providers are in the host Member State where the branch is established.

4.5 For non-card based payment transactions and remote card based payment transactions, 'cross-border payment transaction within the EEA' refers to a payment transaction initiated by a payer, or by or through a payee, where the payer's payment service provider and the payee's payment service provider are located in different Member States.

4.6 For non-remote card-based payment transactions, 'cross-border payment transactions within the EEA' refer to payment transactions where the payer's payment service provider (issuer) and the payee's payment service provider (acquirer) are in different member states or the payer's payment service provider (issuer) is located in a Member State different from that of the POS or ATM.

4.7 'Cross-border payment transactions outside the EEA' refer to payment transactions initiated by a payer, or by or through a payee, where either the payer's or the payee's payment service provider is located outside the EEA while the other is located within the EEA.

4.8 A payment service provider offering payment initiation services should report the executed payment transactions it initiated and the executed fraudulent transactions it initiated in accordance with the following:

a. 'Domestic payment transactions' refer to payment transactions, where the payment initiation service provider and the account servicing payment service provider are located in the same Member State;

b. 'Cross-border payment transactions within the EEA' refer to payment transactions, where the payment initiation service provider and the account servicing payment service provider are located in different Member States;

c. 'Cross-border payment transactions outside the EEA' refer to payment transactions, where the payment initiation service provider is within the EEA and the account servicing payment service provider is located outside the EEA.

Guideline 5: Reporting to the competent authority

5.1. The payment service provider shall report to the competent authority of the home Member State.

5.2. The payment service provider should record data from all its agents, providing payment services in the EEA and aggregate these data with the rest of the data before reporting to the home competent authority. When doing so, the location of the agent is irrelevant for determining the geographical perspective.

5.3. Within the framework of the monitoring and reporting set out in Article 29(2) PSD2 and in Article 40 of Directive 2013/36/EU of the European Parliament and of the Council on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, an established branch of an EEA's payment service provider should report to the competent authority of the host Member State where it is established, separately from the reporting data of the payment service provider in the home Member State.

5.4. When reporting data to the corresponding competent authority, a payment service provider should mention the identification details mentioned in Annex 1.

Guideline 6: Recording/reference dates

6.1 The date to be considered by payment service providers for recording payment transactions and fraudulent payment transactions for the purpose of this statistical reporting is the day the transaction has been executed in accordance with PSD2. In the case of a series of transactions, the date recorded should be the date when each individual payment transaction was executed.

6.2 The payment service provider should report all fraudulent payment transactions from the time fraud has been detected, such as through a customer complaint or other means, regardless of whether or not the case related to the fraudulent payment transaction has been closed by the time the data are reported.

6.3 The payment service provider should report all adjustments to the data referring to any past reporting period at least up to one year old during the next reporting window after the information necessitating the adjustments is discovered. It should indicate that the data reported are revised figures applicable to the past period and should report this revision according to the methodology established by the relevant competent authority.

Guideline 7: Data breakdown

7.1 For e-money payment transactions as defined in Directive 2009/110/EC, the payment service provider should provide data in accordance with Data Breakdown F in Annex 2.

7.2 When providing data on e-money transactions, the payment service provider should include e-money payment transactions

a. where the payer’s PSP is identical to the payee’s PSP, or

b. where a card with an e-money functionality is used.

7.3 The payment service provider for the purpose of e-money payment transactions should report data on volumes and values of all payment transactions, as well as volumes and values of fraudulent payment transactions, with the following breakdowns:

a. geographical perspective,

b. payment channel,

c. authentication method,

d. reason for not applying strong customer authentication (referring to the exemptions to strong customer authentication detailed in chapter 3 of the Regulatory technical standards on strong customer authentication and common and secure communication, Commission Delegated Regulation (EU) 2018/389), and

e. fraud types.

7.4 For money remittance services, the payment service provider should provide data in accordance with Data Breakdown G in Annex 2 and as specified in Guideline 1.3. The payment service provider offering these services should report data on volumes and values of all payment transactions and fraudulent payment transactions in Guideline 2.1 with the geographical perspective.

7.5 When providing provides payment initiation services, the payment service provider should provide data in accordance with Data Breakdown H in Annex 2. The payment service provider should report the executed payment transactions it initiated and the executed fraudulent transactions it initiated, both by volume and value.

7.6 For those payment transactions that qualify for Data Breakdown H in Annex 2, the payment service provider offering payment initiation services should record and report data on volumes and values with the following breakdowns:

a. geographical perspective,

b. payment instrument,

c. payment channel, and

d. authentication method.

7.7 A payment service provider that does not manage the account of the payment service user but issues and executes card-based payments (a card-based payment instrument issuer) should provide data on volumes and values, in accordance with Data Breakdown C and/or E in Annex 2. When such data are provided, the account service payment service provider should ensure that no double-reporting of such transactions occur.

7.8 The payment service provider offering credit transfer and card based payment services should provide data in accordance with Data Breakdowns A, C and/or D in Annex 2, depending on the payment instrument used for a given payment transaction and on the role of the payment service provider. The data include:

a. geographical perspective,

b. payment channel,

c. authentication method,

d. reason for not applying strong customer authentication (referring to exemptions to strong customer authentication detailed in chapter 3 of the RTS on SCA and CSC),

e. fraud types,

f. card function for Data Breakdowns C and D, and

g. payment transactions initiated via a payment initiation service provider for Data Breakdown A.

7.9 The payment service provider should provide data in accordance with Data Breakdown A in Annex 2 for all payment transactions and fraudulent payment transactions executed using credit transfers.

7.10 The payment service provider should provide data in accordance with Data Breakdown B in Annex 2 for all payment transactions and fraudulent payment transactions executed using direct debits. The data include:

a. geographical perspective,

b. channel used for the consent to be given, and

c. fraud types.

7.11 The payment service provider should provide data in accordance with Data Breakdown C in Annex 2 for all payment transactions and fraudulent payment transactions on the issuer side where a payment card was used and the payment service provider was the payer's payment service provider.

7.12 The payment service provider should provide data in accordance with Data Breakdown D in Annex 2 for all payment transactions and fraudulent payment transactions on the acquiring side where a payment card was used and the payment service provider is the payee's payment service provider.

7.13 The payment service provider providing data in accordance with Data Breakdowns A to F in Annex 2 should report all losses due to fraud per liability bearer during the reporting period.

7.14 The payment service provider reporting card payment transactions in accordance with Data Breakdowns C and D in Annex 2 should exclude cash withdrawals and cash deposits.

7.15 The payment service provider (issuer) should provide data in accordance with Data Breakdown E in Annex 2 for all cash withdrawals and fraudulent cash withdrawals through apps, at ATMs, at bank counters and through retailers ('cash back') using a card.

3.2 Guidelines on aggregate fraud data reporting by competent authorities to the EBA and the ECB

Guideline 1: Payment transactions and fraudulent payment transactions

1.1. For the purposes of reporting statistical data on fraud to the EBA and the ECB in accordance with these Guidelines and with Article 96(6) PSD2, the competent authority should report for each reporting period:

a. unauthorised payment transactions made, including as a result of the loss, theft or misappropriation of sensitive payment data or a payment instrument, whether detectable or not to the payer prior to a payment and whether or not caused by gross negligence of the payer or executed in the absence of consent by the payer (‘unauthorised payment transaction’); and

b. 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’).

1.2. For the purposes of Guideline 1.1, the competent authority should report only payment transactions that have been initiated and executed (including acquired where applicable) by payment service providers (including card based payment instrument issuers where applicable). The competent authority should not report data on payment transactions that, however linked to any of the circumstances referred to in Guideline 1.1, have not been executed and have not resulted in a transfer of funds in accordance with PSD2 provisions.

1.3. The competent authority should report all payment transactions and fraudulent payment transactions in accordance with the following:

a. For non-card based payment transactions and remote card based payment transactions, ‘domestic payment transactions’ refer to payment transactions initiated by a payer, or by or through a payee, where the payer’s payment service provider and the payee’s payment service provider are located in the same Member State,

b. For EEA branches, domestic payment transactions refer to the payment transactions where both the payer’s and the payee’s payment service providers are in the host Member State where the branch is established.

c. For non-card based payment transactions and remote card based payment transactions, ‘cross-border payment transactions within the EEA’ refer to payment transactions initiated by a payer, or by or through a payee, where the payer’s payment service provider and the payee’s payment service provider are located in different Member States.

d. For non-remote card-based payment transactions, ‘domestic payment transactions’ refer to payment transactions where the payer’s payment service provider (issuer), the payee’s payment service provider (acquirer) and the POS or ATM used are located in the same Member State. If the payer’s payment service provider and the payee’s payment service provider are in different Member States or the payer’s payment service provider (issuer) is located in a Member State different from that of the POS or ATM, the transaction is a ‘cross-border payment transaction within the EEA’.

e. ‘Cross-border payment transactions outside the EEA’ refer to payment transactions initiated by a payer, or by or through a payee, where either the payer’s or the payee’s payment service provider is located outside the EEA while the other is located within the EEA.

f. ‘Total fraudulent payment transactions’ refer to all the transactions mentioned in Guideline 1.1, regardless of whether the amount of the fraudulent payment transaction has been recovered.

g. ‘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 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.

h. ‘Issuance 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 a fake payment order is issued by the fraudster after having obtained the payer’s/payee's sensitive payment data through fraudulent means.

1.4. Competent authorities should report data from payment service providers offering payment initiation services in accordance with the following:

a. ‘Domestic payment transactions’ refer to payment transactions, where the payment initiation service provider and the account servicing payment service provider are located in the same Member State.

b. ‘Cross-border payment transactions within the EEA’ refer to payment transactions, where the payment initiation service provider and the account servicing payment service provider are located in different Member States.

c. 'Cross-border payment transactions outside the EEA' refer to payment transactions, where the payment initiation service provider is located within the EEA and the account servicing payment service provider is located outside the EEA.

Guideline 2: Data collection and aggregation

2.1. The competent authority should report statistical information on:

a. total payment transactions in line with the different breakdowns in Annex 2 and in accordance with Guideline 1.2; and

b. total fraudulent payment transactions in line with the different breakdowns in Annex 2 and as defined under Guideline 1.3(f).

2.2. The competent authority should report the statistical information in Guideline 2.1 both in volume (i.e. number of transactions or fraudulent transactions) and value (i.e. amount of transactions or fraudulent transactions). It should report volumes and values in actual units, with two decimals for values.

2.3. The competent authority should report the values in euro currency. It should convert data for values of transactions or fraudulent transactions denominated in a currency other than the euro, using the relevant exchange rates applied to these transactions or the average ECB reference exchange rate for the applicable reporting period.

2.4. The competent authority can report zero ('0') where there were no transactions or fraudulent transactions taking place for a particular indicator in the reporting period established.

2.5. The competent authority should aggregate the data collected within its Member State from the addressees of this Guidelines by summing the figures reported for each individual payment service provider in line with the data breakdowns in Annex 2.

2.6. The competent authority should define the secure communication procedures and the format for the reporting of the data by payment service providers. The competent authority should also ensure that an appropriate deadline is given to payment service providers to ensure the quality of the data and to account for the potential delay in reporting fraudulent payment transactions.

2.7. The competent authority should ensure that the data reported under these Guidelines can be cross-referenced and used by the EBA and the ECB in accordance with the data breakdowns in Annex 2.

Guideline 3: Practical data reporting

3.1. The competent authority should report the volumes and values of payment transactions and fraudulent payment transactions in line with Guidelines 2.1 and 2.2. To avoid double counting, data should not be aggregated across the different data breakdowns in Annex 2.

3.2. The competent authority should report adjustments to data on any payment transaction and fraudulent payment transaction reported in any past reporting period during the next reporting window after the information necessitating the adjustments is obtained from given payment service provider(s) and up to 13 months after the transaction was executed (and/or acquired) to enable the payment service user to exercise its right to notify the payment service provider no later than 13 months after the transaction was executed in accordance with Article 71 PSD2.

3.3. The competent authority should at all times ensure the confidentiality and integrity of the information stored and exchanged and the proper identification when submitting data to the ECB and the EBA.

3.4. The competent authority should send the aggregated data to the ECB and the EBA within six months from the day after the end of the reporting period.

3.5. The competent authority should agree with the ECB and the EBA the secure communication procedures and the specific format in which the competent authority should report the data.

Guideline 4: Cooperation among competent authorities

4.1. Where there is more than one competent authority in a Member State under PSD2, the competent authorities should co-ordinate the data collection to ensure that only one set of data is reported for that Member State to the ECB and the EBA.

4.2. Upon request by the competent authority in a home Member State, the competent authority in a host Member State should make available information and data that established branches have reported to them.

Annex 1 – General data to be provided by all reporting payment service providers

General identification data on the reporting payment service provider

Name: full name of the payment service provider subject to the data reporting procedure as it appears in the applicable national register for credit institutions, payment institutions or electronic money institutions.

Unique identification number: the relevant unique identification number used in each Member State to identify the payment service provider, where applicable.

Authorisation number: home Member State authorisation number, where applicable.

Country of authorisation: home Member State where the licence has been issued.

Contact person: name and surname of the person responsible for reporting the data or, if a third party provider reports on behalf of the payment service provider, name and surname of the person in charge of the data management department or similar area, at the level of the payment service provider.

Contact e-mail: email address to which any requests for further clarification should be addressed, if needed. It can be either a personal or a corporate e-mail address.

Contact telephone: telephone number through which any requests for further clarification should be addressed, if needed. It can be either a personal or a corporate phone number.

Data breakdown

All data reported by PSPs using the different breakdowns in Annex 2 should follow the geographical breakdown defined below and should provide both number of transactions *(Actual units, total for the period)* and value of transactions *(EUR/local currency actual units, total for the period)*.

	Value and volume
Area	Domestic; Cross-border *within the EEA; and* Cross-border *outside the EEA*

Annex 2 – Data reporting requirements for payment service providers

A- Data breakdown for credit transfers

	Item	Payment transactions	Fraudulent payment transactions
1	**Credit transfers**	**X**	**X**
1.1	Of which initiated by payment initiation service providers	X	X
1.2	Of which initiated non-electronically	X	X
1.3	Of which Initiated electronically	X	X
1.3.1	Of which initiated via remote payment channel	X	X
1.3.1.1	**Of which authenticated via strong customer authentication**	X	X
	of which fraudulent credit transfers by fraud types:		
1.3.1.1.1	Issuance of a payment order by the fraudster		X
1.3.1.1.2	Modification of a payment order by the fraudster		X
1.3.1.1.3	Manipulation of the payer by the fraudster to issue a payment order		X
1.3.1.2	**Of which authenticated via non-strong customer authentication**	X	X
	of which fraudulent credit transfers by fraud types:		
1.3.1.2.1	Issuance of a payment order by the fraudster		X
1.3.1.2.2	Modification of a payment order by the fraudster		X
1.3.1.2.3	Manipulation of the payer by the fraudster to issue a payment order		X
	of which broken down by reason for authentication via non-strong customer authentication		
1.3.1.2.4	Low value (Art.16 RTS)	X	X
1.3.1.2.5	Payment to self (Art.15 RTS)	X	X

1.3.1.2.6	Trusted beneficiary (Art.13 RTS)	X	X
1.3.1.2.7	Recurring transaction (Art.14 RTS)	X	X
1.3.1.2.8	Use of secure corporate payment processes or protocols (Art. 17 RTS)	X	X
1.3.1.2.9	Transaction risk analysis (Art.18 RTS)	X	X
1.3.2	Of which initiated via non-remote payment channel	X	X
1.3.2.1	**Of which authenticated via strong customer authentication**	X	X
	of which fraudulent credit transfers by fraud types:		
1.3.2.1.1	Issuance of a payment order by the fraudster		X
1.3.2.1.2	Modification of a payment order by the fraudster		X
1.3.2.1.3	Manipulation of the payer by the fraudster to issue a payment order		X
1.3.2.2	**Of which authenticated via non-strong customer authentication**	X	X
	of which fraudulent credit transfers by fraud types:		
1.3.2.2.1	Issuance of a payment order by the fraudster		X
1.3.2.2.2	Modification of a payment order by the fraudster		X
1.3.2.2.3	Manipulation of the payer by the fraudster to issue a payment order		X
	of which broken down by reason for non-strong customer authentication		
1.3.2.2.4	Payment to self (Art.15 RTS)	X	X
1.3.2.2.5	Trusted beneficiary (Art.13 RTS)	X	X
1.3.2.2.6	Recurring transaction (Art.14 RTS)	X	X
1.3.2.2.7	Contactless low value (Art. 11 RTS)	X	X
1.3.2.2.8	Unattended terminal for transport or parking fares (Art. 12 RTS)	X	X

Losses due to fraud per liability bearer:	Total losses
The reporting payment service provider	X
The Payment service user (payer)	X
Others	X

Validation

1.2 + 1.3 = 1; 1.1 does not equate 1 but is a subset of 1
1.3.1 + 1.3.2 = 1.3
1.3.1.1 + 1.3.1.2 = 1.3.1
1.3.2.1 + 1.3.2.2 = 1.3.2
1.3.1.1.1 + 1.3.1.1.2 + 1.3.1.1.3 = fraudulent payment transaction figure of 1.3.1.1; 1.3.1.2.1 + 1.3.1.2.2 + 1.3.1.2.3 = fraudulent payment transaction figure of 1.3.1.2; 1.3.2.1.1 + 1.3.2.1.2 + 1.3.2.1.3 = fraudulent payment transaction figure of 1.3.2.1; 1.3.2.2.1 + 1.3.2.2.2 + 1.3.2.2.3 = fraudulent payment transaction figure of 1.3.2.2
1.3.1.2.4 + 1.3.1.2.5 + 1.3.1.2.6 + 1.3.1.2.7 + 1.3.1.2.8 + 1.3.1.2.9 = 1.3.1.2
1.3.2.2.4 + 1.3.2.2.5 + 1.3.2.2.6 + 1.3.2.2.7 + 1.3.2.2.8 = 1.3.2.2

B – Data breakdown for direct debits

	Item	Payment transactions	Fraudulent payment transactions
2	**Direct debits**	X	X
2.1	Of which consent given via an electronic mandate	X	X
	of which fraudulent direct debits by fraud type:		
2.1.1.1	Unauthorised payment transactions		X
2.1.1.2	Manipulation of the payer by the fraudster to consent to a direct debit		X
2.2	Of which consent given in another form than an electronic mandate	X	X
	of which fraudulent direct debits by fraud type:		
2.2.1.1	Unauthorised payment transactions		X
2.2.1.2	Manipulation of the payer by the fraudster to consent to a direct debit		X

Losses due to fraud per liability bearer:	Total losses
The reporting payment service provider	X
The payment service user (payee)	X
Others	X

Validation

2.1 + 2.2 = 2
2.1.1.1 + 2.1.1.2 = fraudulent payment transaction figure of 2.1
2.2.1.1 + 2.2.1.2 = fraudulent payment transaction figure of 2.2

C- Data breakdown for card-based payment transactions to be reported by the issuer’s payment service provider

	Item	Payment transactions	Fraudulent payment transactions
3	**Card payments (except cards with an e-money function only)**	X	X
3.1	Of which initiated non-electronically	X	X
3.2	Of which initiated electronically	X	X
3.2.1	Of which initiated via remote payment channel	X	X
	of which broken down by card function:		
3.2.1.1.1	Payments with cards with a debit function	X	X
3.2.1.1.2	Payments with cards with a credit or delayed debit function	X	X
3.2.1.2	**Of which authenticated via strong customer authentication**	X	X
	of which fraudulent card payments by fraud types:		
3.2.1.2.1	Issuance of a payment order by a fraudster		X
3.2.1.2.1.1	Lost or stolen card		X
3.2.1.2.1.2	Card not received		X
3.2.1.2.1.3	Counterfeit card		X
3.2.1.2.1.4	Card details theft		X
3.2.1.2.1.5	Other		X
3.2.1.2.2	Modification of a payment order by the fraudster		X
3.2.1.2.3	Manipulation of the payer to make a card payment		X
3.2.1.3	**Of which Authenticated via non-strong customer authentication**	X	X
	of which fraudulent card payments by fraud types:		
3.2.1.3.1	Issuance of a payment order by a fraudster		X
3.2.1.3.1.1	Lost or stolen card		X
3.2.1.3.1.2	Card not received		X
3.2.1.3.1.3	Counterfeit card		X
3.2.1.3.1.4	Card details theft		X

3.2.1.3.1.5	Other		X
3.2.1.3.2	Modification of a payment order by the fraudster		X
3.2.1.3.3	Manipulation of the payer to make a card payment		X
	of which broken down by reason for non-strong customer authentication		
3.2.1.3.4	Low value (Art.16 RTS)	X	X
3.2.1.3.5	Trusted beneficiary (Art.13 RTS)	X	X
3.2.1.3.6	Recurring transaction (Art.14 RTS)	X	X
3.2.1.3.7	Use of secure corporate payment processes or protocols (Art. 17 RTS)	X	X
3.2.1.3.8	Transaction risk analysis (Art.18 RTS)	X	X
3.2.2	Of which initiated via non-remote payment channel	X	X
	of which broken down by card function:		
3.2.2.1.1	Payments with cards with a debit function	X	X
3.2.2.1.2	Payments with cards with a credit or delayed debit function	X	X
3.2.2.2	**Of which authenticated via strong customer authentication**	X	X
	of which fraudulent card payments by fraud types:		
3.2.2.2.1	Issuance of a payment order by a fraudster		X
3.2.2.2.1.1	Lost or stolen card		X
3.2.2.2.1.2	Card not received		X
3.2.2.2.1.3	Counterfeit card		X
3.2.2.2.1.4	Other		X
3.2.2.2.2	Modification of a payment order by the fraudster		X
3.2.2.2.3	Manipulation of the payer to make a card payment		X
3.2.2.3	**Of which authenticated via non-strong customer authentication**	X	X
	of which fraudulent card payments by fraud types:		
3.2.2.3.1	Issuance of a payment order by a fraudster		X
3.2.2.3.1.1	Lost or stolen card		X
3.2.2.3.1.2	Card not received		X
3.2.2.3.1.3	Counterfeit card		X
3.2.2.3.1.4	Other		X
3.2.2.3.2	Modification of a payment order by the fraudster		X
3.2.2.3.3	Manipulation of the payer to make a card payment		X
	of which broken down by reason for non-strong customer authentication		

3.2.2.3.4	Trusted beneficiary (Art.13 RTS)	X	X
3.2.2.3.5	Recurring transaction (Art.14 RTS)	X	X
3.2.2.3.6	Contactless low value (Art.11 RTS)	X	X
3.2.2.3.7	Unattended terminal for transport or parking fares (Art.12 RTS)	X	X

Losses due to fraud per liability bearer:	Total losses
The reporting payment service provider	X
The Payment service user (payer)	X
Others	X

Validation

3.1 + 3.2 = 3
3.2.1 + 3.2.2 = 3.2
3.2.1.1.1 + 3.2.1.1.2 = 3.2.1; 3.2.2.1.1 + 3.2.2.1.2 = 3.2.2
3.2.1.2 + 3.2.1.3 = 3.2.1; 3.2.2.2 + 3.2.2.3 = 3.2.2
3.2.1.2.1 + 3.2.1.2.2 + 3.2.1.2.3 = fraudulent payment transaction figure of 3.2.1.2; 3.2.1.3.1 + 3.2.1.3.2 + 3.2.1.3.3 = fraudulent payment transaction figure of 3.2.1.3; 3.2.2.2.1 + 3.2.2.2.2 + 3.2.2.2.3 = fraudulent payment transaction figure of 3.2.2.2; 3.2.2.3.1 + 3.2.2.3.2 + 3.2.2.3.3 = fraudulent payment transaction figure of 3.2.2.3
3.2.1.2.1.1 + 3.2.1.2.1.2 + 3.2.1.2.1.3 + 3.2.1.2.1.4 + 3.2.1.2.1.5 = fraudulent payment transaction figure of 3.2.1.2.1; 3.2.1.3.1.1 + 3.2.1.3.1.2 + 3.2.1.3.1.3 + 3.2.1.3.1.4 + 3.2.1.3.1.5 = fraudulent payment transaction figure of 3.2.1.3.1; 3.2.2.2.1.1 + 3.2.2.2.1.2 + 3.2.2.2.1.3 + 3.2.2.2.1.4 = fraudulent payment transaction figure of 3.2.2.2.1; 3.2.2.3.1.1 + 3.2.2.3.1.2 + 3.2.2.3.1.3 + 3.2.2.3.1.4 = fraudulent payment transaction figure of 3.2.2.3.1
3.2.1.3.4 + 3.2.1.3.5 + 3.2.1.3.6 + 3.2.1.3.7 + 3.2.1.3.8 = 3.2.1.3; 3.2.2.3.4 + 3.2.2.3.5 + 3.2.2.3.6 + 3.2.2.3.7 = 3.2.2.3

D- Data breakdown for card-based payments transactions to be reported by the acquirer’s payment service provider (with a contractual relationship with the payment service user)

	Item	**Payment transactions**	**Fraudulent payment transactions**
4	**Card payments acquired (except cards with an e-money function only)**	X	X
4.1	Of which initiated non-electronically	X	X
4.2	Of which initiated electronically	X	X
4.2.1	Of which acquired via a Remote channel	X	X
	of which broken down by card function:		
4.2.1.1.1	Payments with cards with a debit function	X	X
4.2.1.1.2	Payments with cards with a credit or delayed debit function	X	X
4.2.1.2	**Of which authenticated via strong customer authentication**	X	X
	of which fraudulent card payments by fraud types:		
4.2.1.2.1	Issuance of a payment order by a fraudster		X
4.2.1.2.1.1	Lost or stolen card		X
4.2.1.2.1.2	Card not received		X
4.2.1.2.1.3	Counterfeit card		X
4.2.1.2.1.4	Card details theft		X
4.2.1.2.1.5	Other		X
4.2.1.2.2	Modification of a payment order by the fraudster		X
4.2.1.2.3	Manipulation of the payer to make a card payment		X
4.2.1.3	**Of which authenticated via non-strong customer authentication**	X	X
	of which fraudulent card payments by fraud types:		
4.2.1.3.1	Issuance of a payment order by a fraudster		X
4.2.1.3.1.1	Lost or stolen card		X
4.2.1.3.1.2	Card not received		X
4.2.1.3.1.3	Counterfeit card		X
4.2.1.3.1.4	Card details theft		X
4.2.1.3.1.5	Other		X

4.2.1.3.2	Modification of a payment order by the fraudster		X
4.2.1.3.3	Manipulation of the payer to make a card payment		X
	of which broken down by reason for non-strong customer authentication		
4.2.1.3.4	Low value (Art.16 RTS)	X	X
4.2.1.3.5	Recurring transaction (Art.14 RTS)	X	X
4.2.1.3.6	Transaction risk analysis (Art.18 RTS)	X	X
4.2.2	Of which acquired via a non-remote channel	X	X
	of which broken down by card function:		
4.2.2.1.1	Payments with cards with a debit function	X	X
4.2.2.1.2	Payments with cards with a credit or delayed debit function	X	X
4.2.2.2	**Of which Authenticated via strong customer authentication**	X	X
	of which fraudulent card payments by fraud types:		
4.2.2.2.1	Issuance of a payment order by a fraudster		X
4.2.2.2.1.1	Lost or stolen card		X
4.2.2.2.1.2	Card not received		X
4.2.2.2.1.3	Counterfeit card		X
4.2.2.2.1.4	Other		X
4.2.2.2.2	Modification of a payment order by the fraudster		X
4.2.2.2.3	Manipulation of the payer to make a card payment		X
4.2.2.3	**Of which authenticated via non-strong customer authentication**	X	X
	of which fraudulent card payments by fraud types:		
4.2.2.3.1	Issuance of a payment order by a fraudster		X
4.2.2.3.1.1	Lost or stolen card		X
4.2.2.3.1.2	Card not received		X
4.2.2.3.1.3	Counterfeit card		X
4.2.2.3.1.4	Other		X
4.2.2.3.2	Modification of a payment order by the fraudster		X
4.2.2.3.3	Manipulation of the payer to make a card payment		X
	of which broken down by reason for non-strong customer authentication		
4.2.2.3.4	Recurring transaction (Art.14 RTS)	X	X
4.2.2.3.5	Contactless low value (Art.11 RTS)	X	X
4.2.2.3.6	Unattended terminal for transport or parking fares (Art.12 RTS)	X	X

Losses due to fraud per liability bearer:	Total losses
The reporting payment service provider	X
The Payment service user (payee)	X
Others	X

Validation

4.1 + 4.2 = 4
4.2.1 + 4.2.2 = 4.2
4.2.1.1.1 + 4.2.1.1.2 = 4.2.1; 4.2.2.1.1 + 4.2.2.1.2 = 4.2.2
4.2.1.2 + 4.2.1.3 = 4.2.1; 4.2.2.2 + 4.2.2.3 = 4.2.2
4.2.1.2.1 + 4.2.1.2.2 + 4.2.1.2.3 = fraudulent payment transaction figure of 4.2.1.2; 4.2.1.3.1 + 4.2.1.3.2 + 4.2.1.3.3 = fraudulent payment transaction figure of 4.2.1.3; 4.2.2.2.1 + 4.2.2.2.2 + 4.2.2.2.3 = fraudulent payment transaction figure of 4.2.2.2; 4.2.2.3.1 + 4.2.2.3.2 + 4.2.2.3.3 = fraudulent payment transaction figure of 4.2.2.3
4.2.1.2.1.1 + 4.2.1.2.1.2 + 4.2.1.2.1.3 + 4.2.1.2.1.4 + 4.2.1.2.1.5 = fraudulent payment transaction figure of 4.2.1.2.1; 4.2.1.3.1.1 + 4.2.1.3.1.2 + 4.2.1.3.1.3 + 4.2.1.3.1.4 + 4.2.1.3.1.5 = fraudulent payment transaction figure of 4.2.1.3.1; 4.2.2.2.1.1 + 4.2.2.2.1.2 + 4.2.2.2.1.3 + 4.2.2.2.1.4 = fraudulent payment transaction figure of 4.2.2.2.1; 4.2.2.3.1.1 + 4.2.2.3.1.2 + 4.2.2.3.1.3 + 4.2.2.3.1.4 = fraudulent payment transaction figure of 4.2.2.3.1
4.2.1.3.4 + 4.2.1.3.5 + 4.2.1.3.6 = 4.2.1.3; 4.2.2.3.4 + 4.2.2.3.5+ 4.2.2.3.6 = 4.2.2.3

E- Data Breakdown for cash withdrawals using cards to be reported by the card issuer’s payment service provider

	Item	Payment transactions	Fraudulent payment transactions
5	**Cash withdrawals**	X	X
	Of which broken down by card function		
5.1	Of which payments with cards with a debit function	X	X
5.2	Of which payments with cards with a credit or delayed debit function	X	X
	of which fraudulent card payments by fraud types:		
5.2.1	Issuance of a payment order (cash withdrawal) by the fraudster		X
5.2.1.1	Lost or stolen card		X
5.2.1.2	Card not received		X
5.2.1.3	Counterfeit card		X
5.2.1.4	Other		X
5.2.2	Manipulation of the payer to make a cash withdrawal		X

Losses due to fraud per liability bearer:	Total losses
The reporting payment service provider	X
The Payment service user (account holder)	X
Others	X

Validation

5.1 + 5.2 = 5
5.2.1 + 5.2.2 = 5
5.2.1.1 + 5.2.1.2 + 5.2.1.3 + 5.2.1.4 = 5.2.1

F – Data Breakdown to be provided for e-money payment transactions

	Item	**Payment transactions**	**Fraudulent payment transactions**
6	**E-money payment transactions**	**X**	**X**
6.1	**Of which via remote payment initiation channel**	X	X
6.1.1	**of which authenticated via strong customer authentication**	X	X
	of which fraudulent e-money payment transactions by fraud types:		
6.1.1.1	Issuance of a payment order by the fraudster		X
6.1.1.2	Modification of a payment order by the fraudster		X
6.1.1.3	Manipulation of the payer by the fraudster to issue a payment order		X
6.1.2	**of which authenticated via non-strong customer authentication**	X	X
	of which fraudulent e-money payment transactions by fraud types:		
6.1.2.1	Issuance of a payment order by the fraudster		X
6.1.2.2	Modification of a payment order by the fraudster		X
6.1.2.3	Manipulation of the payer by the fraudster to issue a payment order		X
	of which broken down by reason for non-strong customer authentication		
6.1.2.4	Low value (Art.16 RTS)	X	X
6.1.2.5	Trusted beneficiary (Art.13 RTS)	X	X
6.1.2.6	Recurring transaction (Art.14 RTS)	X	X
6.1.2.7	Payment to self (Art. 15 RTS)	X	X
6.1.2.8	Use of secure corporate payment processes or protocols (Art. 17 RTS)	X	X
6.1.2.9	Transaction risk analysis (Art.18 RTS)	X	X
6.2	**Of which via non-remote payment initiation channel**	X	X
6.2.1	**Of which authenticated via strong customer authentication**	X	X
	of which fraudulent e-money payment transactions by fraud types:		
6.2.1.1	Issuance of a payment order by the fraudster		X
6.2.1.2	Modification of a payment order by the fraudster		X

6.2.1.3	Manipulation of the payer by the fraudster to issue a payment order		X
6.2.2	**Of which authenticated via non-strong customer authentication**	X	X
	of which fraudulent e-money payment transactions by fraud types:		
6.2.2.1	Issuance of a payment order by the fraudster		X
6.2.2.2	Modification of a payment order by the fraudster		X
6.2.2.3	Manipulation of the payer by the fraudster to issue a payment order		X
	of which broken down by reason for non-strong customer authentication		
6.2.2.4	Trusted beneficiary (Art.13 RTS)	X	X
6.2.2.5	Recurring transaction (Art.14 RTS)	X	X
6.2.2.6	Contactless low value (Art.11 RTS)	X	X
6.2.2.7	Unattended terminal for transport or parking fares (Art.12 RTS)	X	X

Losses due to fraud per liability bearer:	Total losses
The reporting payment service provider	X
The Payment service user	X
Others	X

Validation

6.1 + 6.2 = 6
6.1.1 + 6.1.2 = 6.1; 6.2.1 + 6.2.2 = 6.2
6.1.1.1 + 6.1.1.2 + 6.1.1.3 = fraudulent payment transaction figure of 6.1.1; 6.1.2.1+ 6.1.2.2 + 6.1.2.3 = fraudulent payment transaction figure of 6.1.2; 6.2.1.1 + 6.2.1.2 + 6.2.1.3 = fraudulent payment transaction figure of 6.2.1; 6.2.2.1 + 6.2.2.2 + 6.2.2.3 = fraudulent payment transaction figure of 6.2.2
6.1.2.4 + 6.1.2.5 + 6.1.2.6 + 6.1.2.7 + 6.1.2.8 + 6.1.2.9 = 6.1.2; 6.2.2.4 + 6.2.2.5 + 6.2.2.6 + 6.2.2.7 = 6.2.2

G – Data breakdown to be provided for money remittance payment transactions

	Item	Payment transactions	Fraudulent payment transactions
7	**Money remittances**	X	X

H – Data breakdown for transactions initiated by payment initiation services providers

	Item	Payment transactions	Fraudulent payment transactions
8	**Payment transactions initiated by payment initiation service providers**	**X**	**X**
8.1	Of which initiated via remote payment channel	X	X
8.1.1	Of which authenticated via strong customer authentication	X	X
8.1.2	Of which authenticated via non-strong customer authentication	X	X
8.2	Of which initiated via non-remote payment channel	X	X
8.2.1	Of which authenticated via strong customer authentication	X	X
8.2.2	Of which authenticated via non-strong customer authentication	X	X
	of which broken down by payment instrument		
8.3.1	Credit transfers	X	X
8.3.2	Other	X	X

Validation

8.1 + 8.2 = 8
8.3.1 + 8.3.2 = 8
8.1.1 + 8.1.2 = 8.1
8.2.1 + 8.2.2 = 8.2