BANCO DE ESPAÑA
Eurosistema

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

(EBA/GL/2018/05)

These Guidelines from the European Authority Banking (EBA) are addressed to competent authorities, as defined in point (i) of Article 4(2) of Regulation (EU) nº 1093/2010, and 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.

The aim of these Guidelines is to 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 these authorities have to share with the EBA and the ECB, in accordance with Article 96(6) of Directive (EU) 2015/2366 (PSD2).

These Guidelines have been developed by the EBA in accordance with article 16 of Regulation (EU) nº 1093/2010. The EBA published the English version of these Guidelines on 18 July 2018 and the Spanish version was released on 17 September 2018.

The guidelines apply from 1 January 2019, with the exception of the reporting of data related to the exemptions to the requirement to apply 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 Executive Commission of the Bank of Spain, in its capacity as the competent authority for the direct supervision of payment service providers, has adopted the Guidelines EBA/GL/2018/05 as their own on 21 March 2020.

EBA/GL/2018/05

18 July 2018

Final Report

Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2)

Contents

1. Executive Summary 3
2. Abbreviations 4
3. Background and rationale 5
4. Guidelines 11
5. Accompanying documents 44
5.1 Cost benefit analysis 44
5.2 Feedback on the public consultation and on the opinion of the BSG 51

1. Executive Summary

Directive (EU) 2015/2366 on payment services in the internal market (Payment Services Directive 2 – PSD2) entered into force in the European Union (EU) on 12 January 2016 and applies since 13 January 2018. One of the PSD2 requirements applicable to all payment service providers (PSPs) relates to the reporting of fraud data on means of payment. More specifically, Article 96(6) PSD2 states that PSPs must provide 'statistical data on fraud relating to different means of payment to their competent authorities' and that the competent authorities (CAs) must, in turn, 'provide EBA and the ECB with such data in an aggregated form'.

In order to ensure that these high-level provisions are implemented consistently among Member States and that the aggregated data provided to the EBA and the ECB are comparable and reliable, the EBA, in close cooperation with the ECB, is proposing two sets of Guidelines (GL) on the reporting requirements of fraudulent payment transactions. On 2 August 2017, the EBA published a consultation paper (CP) and the consultation period closed on 3 November 2017. The EBA received 48 responses to the CP representing a wide range of market participants, regulated and unregulated. The EBA, in close cooperation with the ECB, has assessed the responses and identified approximately 200 different issues or requests for clarification that respondents had raised.

The EBA agreed with some of these proposals, and their underlying rationale, and has made a number of changes to the GL and related annexes as a result. This includes the requirements in relation to the reporting frequency, which the EBA has changed from a set of data on a quarterly frequency and a more detailed set of data on a yearly frequency to one set of data on a semi-annual frequency. The geographical area, too, has been reduced to the same area for all of the requirements in the GL (with no country-by-country data requirement), and the number of categories of fraudulent transactions to be reported has been reduced from three to two, with fraudulent transactions where the payer is the fraudster now no longer within the scope of the GL. Finally, the fraud types have been aligned across the payment services and instruments. The other requirements proposed in the CP remain unchanged, including the exclusion of account information service providers from the fraud statistics reporting obligations.

The EBA has in addition made particular efforts, together with the ECB, to further align the GL with other similar reporting instruments mentioned by the respondents, in particular with the ECB Regulation on payment statistics (ECB/2013/43) applicable to PSPs within the euro area and the complementary ECB Recommendation on payment statistics (ECB/2013/44) addressed to non-euro area national central banks.

Next steps

The GL will be translated into the official EU languages and published on the EBA website. The deadline for CAs to report whether they comply with the GL will be two months after the publication of the translations. The GL will apply from 1 January 2019.

2. Abbreviations

AISP	Account Information Service Provider
ASPSP	Account Servicing Payment Service Provider
ATM	Automated Teller Machine
CA	Competent Authority
BSG	Banking Stakeholder Group
CBPII	Card-Based Payment Instruments Issuer
CP	Consultation Paper
CPMI	Committee on Payments and Market Infrastructures
CSC	Common and Secure open standards for Communication
EBA	European Banking Authority
ECB	European Central Bank
EEA	European Economic Area
EMD	Electronic Money Directive
EMI	Electronic Money Institution
ESCB	European System of Central Banks
EU	European Union
GL	Guidelines
MS	Member State(s)
PI	Payment Institution
PISP	Payment Initiation Service Provider
POS	Point Of Sale
PSD	Payment Services Directive
PSP	Payment Service Provider
PSU	Payment Service User
RTS	Regulatory Technical Standards
SCA	Strong Customer Authentication

3. Background and rationale

3.1 Background

1. Directive (EU) 2015/2366 on payment services in the internal market (Payment Services Directive 2 – PSD2) entered into force on 12 January 2016 and applies since 13 January 2018. One of the objectives of PSD2 is to ensure the security of electronic payments and 'to reduce, to the maximum extent possible, the risk of fraud' (recital 95).

2. More specifically, Article 96(6) PSD2 provides that 'Member States shall ensure that payment service providers provide, at least on an annual basis, statistical data on fraud relating to different means of payment to their competent authorities (CAs). Those CAs shall provide EBA and the ECB with such data in an aggregated form'.

3. Not all Member States (MS) currently collect fraud data for all payment instruments, and those that do tend to use different definitions of what a fraudulent payment transaction is, different methodologies and/or different data breakdowns. In particular, MS that currently *do* collect fraud data either do not cover transactions using all payment instruments or transactions made through all types of payment service providers (PSPs) within their jurisdiction, or the data categories and/or level of detail differs.

4. The European System of Central Banks (ESCB), in its function as overseer of payment schemes and instruments, collects fraud data too, but those data are limited to card payments and based on non-legally binding reporting requirements. Additional payment statistics are collected by the ECB, with the assistance of the euro area national central banks, from euro area PSPs and these include data on all means of payments but do not, at the moment, include reporting of data related to fraudulent payment transactions.[1]

5. Against this background, the EBA, in close cooperation with the ECB, has developed two sets of Guidelines (GL) on fraud data reporting requirements. The two GL aim to ensure that the high-level provisions in Article 96(6) PSD2 are implemented consistently across the MS of the European Union (EU) and the European Economic Area (EEA) and that the aggregated data provided to the EBA and the ECB are comparable and reliable.

6. The first set of GL is addressed to PSPs while the second is addressed to CAs. The first set of GL sets out requirements applicable to all PSPs, with the exception of account information service providers (AISPs) [2], while the second set of GL sets out requirements on providing data in an aggregate form to the ECB and the EBA that are applicable to CAs.

7. On 2 August 2017, the EBA published a consultation paper (CP) for a three-month consultation period. The EBA received 48 responses to the CP representing a wide range of market participants, including PSPs, merchants and technology service providers.

[1] See ECB *Regulation of the European Central Bank of 28 November 2013 on payments statistics*, ECB/2013/43

[2] PSPs that provide only account information services, but no other payment services, as referred to in Article 33 of PSD2

8. The EBA, in close cooperation with the ECB, has reviewed and assessed the responses, and has identified in the process approximately 200 different issues or requests for clarification that respondents had raised. Section 3.2 presents an assessment of the four main concerns that were raised, while the feedback table in section 5.2 provides an exhaustive and comprehensive assessment of *all* of the comments that the EBA received and any changes that the EBA decided to make to the GL as a result, where applicable. Section 4, in turn, presents the final GL themselves.

3.2 Rationale

9. Overall, the respondents supported the EBA developing these GL to provide a consistent approach and a level-playing field for all PSPs across all MS.

10. The main concerns that arose during the consultation and that resulted in the EBA making changes to the GL related to: (1) the objectives and the alignment with other instruments, (2) the categories of fraudulent transactions to be reported, (3) the scope and addressees of the GL and (4) the reporting burden (regarding frequency, application date and detailed data breakdown).

Objectives and the alignment with other instruments

11. The respondents generally agreed with the objectives listed in the CP but stated that it was unclear whether a direct link between these GL and the Regulatory technical standards on strong customer authentication and common and secure open standards for communication (RTS on SCA and CSC) existed or not. Some supported such a link while others did not, putting forward arguments accordingly.

12. The EBA considered these arguments and arrived at the view that the GL are a tool for supervisors to monitor compliance with PSD2 itself and the technical standards and GL that the EBA has developed in support of the directive, including the RTS on SCA and CSC. Most of the respondents who raised this issue specifically queried whether or not there was a link between the GL and the calculation of the fraud rate for the purpose of the transaction-risk analysis (TRA) exemption under Article 18 of the RTS on SCA and CSC. The EBA clarifies that the GL and the RTS on SCA and CSC are aligned to the extent that the same two categories included in the reporting for the purpose of the EBA GL, namely unauthorised transactions and transactions as a result of the manipulation of the payer, should be used to calculate the fraud rate as explained in paragraph 46 of the EBA Opinion published on 13 June 2018.

13. In addition, a number of respondents queried the link between the EBA GL and the ECB Regulation on payment statistics (ECB/2013/43). On the basis of Article 96(6) PSD2, which refers to both the ECB and the EBA, the objectives of the draft GL included an objective for the ESCB oversight of payment schemes and instruments. In parallel, the ECB is currently reviewing its Regulation and has for that purpose conducted a fact-finding exercise. This review is exploring, inter alia, whether the scope of the Regulation can be extended to include fraud statistics to serve the ESCB's oversight function. In view of this development, the EBA has concluded that the EBA GL should be primarily a tool for the purpose of supervision and that therefore the data required to be reported should be suitable and necessary for those purposes. As a result, the EBA GL no longer require the reporting of data that are *solely* relevant for oversight purposes.

14. This means that it is envisaged that the regulatory requirements related to fraud reporting consist of two components: (i) the EBA GL, which focus on the reporting of data that are relevant mostly for supervisory purposes, which will become applicable from January 2019 and (ii) an appropriate ESCB regulatory tool to outline oversight-only reporting requirements for fraud data on means of payment (e.g. potentially a revised ECB Regulation on payment statistics).

15. The EBA, in close cooperation with the ECB, has endeavoured to ensure that the methodology, definitions, fraud types and categories that are specified in the EBA GL when requiring reporting of the same payment data are consistent with other reporting instruments (e.g. the ECB Regulation on payment statistics), thus minimising the reporting burden on PSPs.

16. The EBA may wish at a later stage to publish aggregate and anonymised statistical data (i.e. not containing any confidential information).

Categories of fraudulent transactions to be reported

17. Some respondents disagreed with the inclusion of 'manipulation of the payer' and 'payer acting fraudulently' in addition to 'unauthorised transactions' within the total of 'fraudulent payment transactions', arguing that these data were unreliable or that such fraud was not within the control of PSPs and therefore should not be reported by them. The EBA considered these arguments and arrived at the view that, while it is important to have a complete and accurate picture of payment fraud, fraud that is completely outside of the control of PSPs should not be included, as it is of limited relevance and interest to the supervisors of PSPs (although it may be relevant for other authorities, including law enforcement). The EBA has therefore concluded that the category 'payer acting fraudulently' should be excluded.

18. By contrast, and although the reporting of data under the category of 'fraud by manipulation of the payer' may not be completely reliable yet, the EBA is of the view that such fraud cases are caused by a third party manipulating a payer into making a payment and that it is, at least partially, the responsibility of the PSP to identify any such potential case. This is particularly the case with regard to the use of transaction monitoring systems, and in particular TRA. This is of particular concern to the EBA, given that this type of fraud has significantly increased in recent years, suggesting that fraudsters may be shifting to this *modus operandi*. Therefore PSPs and CAs will need to report data to this category alongside data in the category of unauthorised transactions.

19. In addition, and in line with suggestions from a number of respondents, the two categories mentioned above have been aligned with fraud types and sub-types detailed in Annex 2.

20. Regarding the reporting of fraudulent payment transactions in the context of direct debits, the EBA clarifies that refunds under eight weeks should not be automatically reported, as they do not always indicate fraud cases; such transactions should be reported only if they were subject to fraud and the reporting PSP was aware that this was the case, without implying any legal obligation to ask the payment service user whether this was the case.

Scope and addressees

21. A significant number of respondents disagreed with the proposal in the CP not to include registered AISPs. Some respondents suggested that these providers should also be monitoring fraud and that, as new providers, it was important for them to report. However, most respondents agreed that these providers could not report any fraudulent payment transactions data and that including them would therefore require a change in the scope of the GL, which is limited to fraudulent payment transactions.

22. Having assessed these responses, the EBA remains of the view that, for the purpose of these GL, registered AISPs remain excluded from the requirement to report on 'means of payment' in accordance with Article 96(6) PSD2. For overall supervisory purposes, statistical data from registered AISPs may be relevant to CAs, independently from this reporting.

23. When developing the CP, the EBA had not specifically considered card-based payment instrument issuers (CBPIIs). Having assessed the responses received and having considered the business models of CBPIIs, the EBA has concluded that CBPIIs, too, should report under the card issuer Data Breakdowns C and E in Annex 2 of the GL.

24. A number of respondents also queried if sub-acquirers or acquirers should report. Again, the EBA has assessed the responses received and has concluded that the acquirer that has the contract with the payment service user is the one required to report the transaction and that transactions should be reported under Data Breakdown D on card acquiring.

25. With regard to the scope of the GL, the draft CP included both gross and net fraud. Many respondents were critical of the inclusion of net fraud. They criticised the definition used as well as questioning the practical implementation and raising methodological issues related to calculating net fraud figures. Many of these respondents also disagreed that the inclusion of net fraud would provide CAs, the EBA and the ECB with the information they sought, namely where the responsibility lay and consequently who had borne the losses. They also suggested it was more a prudential measure than a data reporting one, and therefore not relevant to these GL.

26. The EBA has assessed the strength of the arguments put forward and has arrived at the conclusion that net fraud should be removed from the GLs. Instead, the GLs now require PSPs to report the general value of losses borne by them and by the relevant payment service user. Losses borne are understood as the residual loss that is finally registered in the PSP's books after any recovery of funds has taken place. This differs from net fraud because the EBA expects one single figure for any given period, unrelated to the payment transactions reported during that period. Since refunds by insurance agencies are not related to fraud prevention for the purposes of PSD2, the final fraud loss figures should not take into account such refunds. The GL require PSPs to report losses that have been recorded in their books due to fraud during the period of reporting, irrespective of the transactions reported during that period. Such losses are independent and separate and should be reported under a separate heading from the rest of the data.

27. The EBA also remains of the view that with the exception of data from branches established in other MS, which should be reported by said branches to the host CA, all other data should be reported by the PSPs to their home CA, including payment transaction data from agents.

28. Finally, following the consultation and the responses received, the GL, in line with a request put forward by many respondents, continue to exclude attempted fraud data and make no distinction between consumer and corporate transactions.

Reporting burden: frequency of reporting, date of application and level of detail

29. Many respondents commented on the reporting burden placed on PSPs by the GL, in particular for those PSPs that do not currently report under the ECB Regulation on payment statistics. A number of respondents were of the view that the burden was disproportionate, in terms of both the frequency of reporting and the level of detail required. This led a large number of respondents to argue that it would be particularly challenging to have such reporting up and running from H2 2018 as proposed in the CP.

Frequency

30. Many respondents were critical of quarterly reporting, for example because of the administrative burden of reporting so frequently. These respondents suggested semi-annual or annual reporting instead. A number of respondents also disagreed with reporting different data in terms of granularity depending on the frequency of the reporting and were of the view that reporting the same data at all times would be preferable.

31. The EBA assessed these views and agreed with a number of respondents who suggested reporting the same detailed data, rather than different sets of data with different frequencies, and decided to require that such data be reported on a semi-annual basis. The EBA considers this to be an appropriate compromise, limiting the burden for PSPs and CAs on the one hand and taking into account the need for the EBA and the ECB to have access to relatively timely data on the other.

32. The GL foresee an exception to this rule for the small Payment Institutions (PIs) and Electronic money Institutions (EMIs) that, under the national transposition of Article 32 PSD2 and Article 9 of the Electronic money Directive (EMD), would be able to benefit from an exemption. These PSPs would need to report only annually with a half-yearly breakdown. This has led to changes to GL 3.1, 3.2 and 7 in the set of GL addressed to PSPs. CAs have to provide data to the ECB and the EBA within six months after the end of the reporting period, irrespective of whether that period is semi-annual (for most PSPs) or annual (for small PIs and EMIs). The GL do not specify the timeline for PSPs to provide data to CAs, given that CAs use different methodologies and timelines in their existing payment statistics collection.

Date of application

33. Related to the above, many respondents also suggested that collecting and reporting the required data would not be possible immediately after the date of application of the GL and argued that they needed to adapt their systems, noting the delay in publishing the GL themselves.

34. The EBA considers these arguments to be valid and has therefore agreed to postpone the first reporting period. Given the changes expected from market participants (and in particular from those that are not yet collecting payment data under the ECB Regulation on payment statistics), the detailed data breakdowns and the implementation work required, the EBA has decided to

change the GL so that they now require the data collection to start in January 2019, with the exception of the data breakdown on exemptions used when SCA was not applied, for which data collection will start only from the date of application of the RTS on SCA and CSC on 14 September 2019. The EBA clarifies that fraudulent transactions should be assigned to a specific exemption and thus reported under one exemption only, even though in theory more than one exemption could have been applicable. This means that the sum of the data reported under non-SCA exemption fields should equal the total provided separately under non-SCA field.

35. This means that the first reporting period will be H1 2019 for CAs to report data on to the ECB and the EBA by the end of 2019. This will ensure that consistent and comparable data are collected ahead of the date of application of the RTS on SCA and CSC for CAs and will enable the EBA to compare the evolution of fraud across payment services and instruments. This has led to a change in the date of application in paragraph 14 of the GL under the heading 'Date of application' (page 16 of this document).

36. The obligation under Article 96(6) PSD2 applies from the time PSD2 is transposed in any given MS. This means that, for the period between 13 January 2018 (or the date of application of the national legislation transposing PSD2 if this is later) and 31 December 2018, PSPs will not be required to report the data foreseen under the EBA GL.

Level of detail

37. A number of respondents had queries about the geographical breakdown and expressed confusion because there did not seem to be a full alignment with the ECB Regulation on payment statistics. A large number of respondents also disagreed with the need for country-level data for a large number of the data breakdowns proposed in the CP. The EBA has assessed the concerns raised and has decided to simplify the geographical reporting.

38. Given that the aim of these GL is to provide a tool mostly for supervisors and regulators, the EBA concluded that there was no strong need for the GL to include country-by-country data. Instead, the revised EBA GL require a geographical breakdown only between domestic, cross-border within the EEA and cross-border outside of the EEA.

39. Furthermore, the EBA has assessed the responses commenting that the level of data proposed in the CP was overly burdensome and has arrived at the view that the GL should be changed so as no longer to include breakdowns under 'non-electronic transactions'.

40. The updated GL have also simplified the reporting of data breakdowns for money remittance and PISPs and have as a result amended Data breakdowns G and H respectively. Finally, the EBA has deleted the data breakdown on 'reason for applying SCA' while adding the category 'card details theft' for card payments. Other changes are highlighted in the feedback table under Section 5.2 (Pages 54 to 134).

4. Guidelines

EBA/GL/2018/05

18 July 2018

Guidelines

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

Version of the guidelines updated on 20/12/2018 to reflect editorial changes applied to pages 15, 38, 40 and 41

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[3]. 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/2018/05'. 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).

[3] 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

5. Accompanying documents

5.1 Cost-benefit analysis

Article 16(2) of the EBA Regulation provides that the EBA should carry out an analysis of 'the potential related costs and benefits' of any GL it develops. This analysis should provide an overview of the findings regarding the problem to be dealt with, the solutions proposed and the potential impact of these options'.

A. Problem identification and baseline scenario

PSD2 provides a set of rules in order to enhance transparency, security, efficiency and confidence within the EU/EEA-wide single market for payments. The Directive updated the existing rules with a view to creating a more effective regulatory framework for payment services.

In particular, one of the objectives of the Directive is to improve the protection of consumers by reducing the risk of fraud and other payment-related problems.

In view of the above, Article 96(6) PSD2 states that 'Member States shall ensure that payment service providers provide, at least on an annual basis, statistical data on fraud relating to different means of payment to their CAs. Those CAs shall provide the EBA and the ECB with such data in an aggregated form'.

The growth of innovative payment services in recent years raises concerns about the way in which consumer data are used by PSPs; consumers' lack of understanding of security risks when inputting personal information; and, for the purpose of payments, weak authentication requirements established by merchants or PSPs, which can result in a significant rise in fraud or alleged fraud.[4]

The security of payment services plays a key role in fostering the exchange of goods and services within the EU single market. Consumers are particularly sensitive to payment security issues[5] and the development of the European payment services market will depend to a great extent on the level of safety and confidence among the stakeholders involved.

The current framework for fraud data reporting is fragmented and differs across the EU. Not all MS collect data on payment services in the same way. Differences include the different definitions of 'fraudulent payment transaction' used across countries and different reporting methodologies applied. Moreover, the level of detail varies widely across the EU.

[4] EBA Consumer Trends Report 2016,
http://www.eba.europa.eu/documents/10180/1360107/Consumer+Trends+Report+2016.pdf

[5] European Commission, Green Paper: Towards an integrated European market for card, internet and mobile payments, 11 January 2012.

In conclusion, the lack of uniform and effective fraud data reporting covering all payment services and instruments within the EU could result in an uneven playing field across MS and could also adversely affect consumer protection against fraud as a result of weak monitoring activity.

B. Policy objectives

These GL aim to ensure that the reporting of fraud data by PSPs to CAs is comparable and reliable within all MS and at EU level. This will contribute to enhancing consumer protection, promoting innovation and improving the security of electronic payment services across the EU[6] and the EEA.

Analysing and comparing fraud data on different PSPs, payment instruments and services will contribute to assessing the effectiveness of applicable regulations, identifying fraud trends and potential risks and informing any future regulatory or supervisory change or action.
The recording of fraud data should also enable PSPs to better assess security incidents or emerging fraud trends and threats and contribute to monitoring fraud, including by type of service and payment instrument.

Furthermore, if the aggregate and anonymised information were to be published, consumers would have access to reliable and up-to-date data providing a good illustration of the current state of payment frauds within the EU and the EEA, which could in turn increase the level of confidence in the payment services market.

C. Options considered and preferred options

The EBA GL contain two sets of GL: GL applicable to PSPs and GL applicable to CAs. Each is considered in turn.

GL on fraud data reporting applicable to PSPs

Guideline 2: General data requirements

PSPs could report the information in accordance with the following options:

- Option 2.1.1: providing fraudulent payment transaction data only;
- Option 2.1.2: providing data on fraudulent payment transactions as well as total payment transactions;
- Option 2.1.3: providing data on fraudulent payment transactions, attempted fraudulent payment transactions and total payment transactions.

Option 2.1.1 would be less costly for both services providers and CAs.
Data on total transactions, however, are essential to understand the relative dimension of the information to be reported, compile percentages and make comparisons. Option 2.1.2 addresses

[6] EBA Annual Report 2015, http://www.eba.europa.eu/documents/10180/1495214/EBA+Annual+report+2015.pdf/9bd71d6b-002f-4b8b-8ff5-d7b85238f8d8

this issue, although it may entail higher costs than Option 2.1.1. The EBA notes, however, that most providers should already be recording at least some of these data.
Option 2.1.3 would imply the highest compliance costs and it could also make the assessment of the information more complicated compared with the other options due to the amount of data to be provided and recorded.

Option 2.1.2 has been selected.

Alternative options have been also considered with regard to the type of fraudulent payment transactions data to be provided:

- Option 2.2.1: providing only gross fraudulent payment transactions data;
- Option 2.2.2: providing gross and net fraudulent payment transactions data;
- Option 2.2.3: providing gross fraudulent payment transactions data, limiting the net data to only the amount of a transactions that has been recovered by the reporting PSPs (excluding other parties to the payment chain recovering part of the amount);
- Option 2.2.4: Providing gross fraudulent payment transactions data with high-level losses data across the given reporting period.

Option 2.2.1 would not allow CAs to understand and assess the responsibilities of the different PSPs that were part of the payment chain.
Option 2.2.2 would somewhat address this issue by adding net fraudulent payment data. However, any given PSP would not be able to know the overall net figure for any given payment transaction. The PSP would mostly be able to provide data with regard to whether it had been able to recover some of the funds.
Option 2.2.3 takes this practical challenge into account, requiring providers to report only data on funds that they have been able to recover. This would allow CAs to get some understanding of the amount recovered. However, it would not enable CAs to form a reliable view on the allocation of responsibilities and would, rather, provide information of a prudential nature, focusing on exposure.
Option 2.2.4, by requiring the reporting of data on high-level losses in addition to fraudulent payment transactions data would enable CAs to understand and assess the responsibility of the reporting provider. Delinking the losses figures from specific transactions provides a solution to the weaknesses identified in options 2.2.2 and 2.2.3.

Option 2.2.4 has been selected.

<u>Guideline 3: Frequency and reporting timelines</u>

PSPs could report the data required with the following frequencies:

- Option 3.1: all data are reported quarterly;
- Option 3.2: all data are reported annually;

- Option 3.3: high level data are reported quarterly and detailed data are reported annually for all PSPs, except for small PSPs[7]; or
- Option 3.4.: all data are reported semi-annually by all PSPs, except for small PSPs.

According to Article 96(6) PSD2, 'Member States shall ensure that payment service providers provide, at least on an annual basis, statistical data on fraud relating to different means of payment to their competent authorities'. This means that PSD2 does not prevent reporting more frequently than annually.
In order to enable CAs to act quickly, it is reasonable to require some data more frequently than annually.
However, Option 3.1 is considered infeasible, as it would entail excessively high compliance costs for PSPs and CAs.
Option 3.2 is also considered infeasible as it would prevent CAs from acting quickly and prevent the identification of any potential issue before it worsened.
Option 3.3 complies with Article 96(6) PSD2 and is more proportionate but it brings a degree of complexity by requiring different types of data depending on frequency, which may be costly and cumbersome to implement.
Option 3.4 complies with Article 96(6) PSD2, and is more proportionate than Option 3.1 as well as simpler and more straightforward to implement. Furthermore, Option 3.4 is consistent with the proportionality principle as it excludes some small PSPs from reporting data more frequently than on an annual basis.

Option 3.4 has been selected.

Guideline 4: Geographical breakdown and reporting

PSPs could report the data required in accordance with the following geographical breakdowns:

- Option 4.1.1: PSPs do not provide any geographical breakdown;
- Option 4.1.2: PSPs distinguish only between transactions within the EEA and cross-border outside the EEA;
- Option 4.1.3: PSPs distinguish between domestic, cross border within the EEA and cross-border outside the EEA.
- Option 4.1.4: PSPs break the data down country by country.

Option 4.1.1 does not provide any information about cross-border payments. This option would not allow CAs to understand where frauds originate. Option 4.1.4 would be very burdensome on providers and not proportionate to the supervisory objective of the GL.
Options 4.1.2 and 4.1.3 provide important information about the value and volume of cross-border payments. However, Option 4.1.2 would provide a more limited picture of the issue addressed in Guideline 4 than would Option 4.1.3.

Option 4.1.3 has been selected.

[7] Payment service providers that may benefit from an exemption under Article 32 PSD2 and e-money institutions that may 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 full set of data requested under the applicable form(s) under Annex 1 on an annual basis.

Guideline 5: Reporting to the competent authority

PSPs could report the data required in accordance with the following geographical reporting options:

- Option 5.1.1: PSPs, including all established branches and agents, report all data to the home MS.
- Option 5.1.2: established branches outside the home MS report data separately to the host Member State and PSPs report data excluding data from established branches but including data from agents to their home Member State;
- Option 5.1.3: established branches outside the home MS and agents report data separately to their host Member State and PSPs report data excluding data from established branches and agents to their home Member State.

Option 5.1.1 would not provide accurate information on the number of payment transactions in each MS given that all transactions are reported to the home authority regardless of where their main business is conducted (which might be through branches outside of the home authority's territory). Options 5.1.2 and 5.1.3 are both better able to represent the current status of payment transactions in each MS. Nevertheless, it is reasonable to assume that Option 5.1.3 would be excessively costly and difficult to apply for CAs and PSPs alike. In addition, agents are not authorised by CAs and would not be able to separately report to host authorities under the EU legislative framework.

Option 5.1.2 has been selected.

Guideline 6: Reporting dates

PSPs could report all fraudulent payment transactions in accordance with the following options for reporting dates:

- Option 6.1: fraudulent payment transactions are reported for the reporting period in which fraud is detected;
- Option 6.2: fraudulent payment transactions are reported for the reporting period in which a case is closed.

Option 6.1 would allow PSPs to report timely and fairly accurate data. In contrast, Option 6.2 could entail significant delays in reporting cases of fraudulent payment transaction.

Option 6.1 has been selected.

Guideline 7: Detailed data breakdown

PSPs could report the data required at the following levels of detail:

- Option 7.1: data breakdowns that differ depending on services and payment instruments used apply;
- Option 7.2: the same data breakdown applies for all;
- Option 7.3: the lowest common denominator of data detail applies.

Option 7.1 is consistent with the proportionality principle and would address the potential unavailability of data to some PSPs.

In contrast, Option 7.2 would not be feasible due to the inability of all PSPs to report data at the same level of detail. This option would also entail higher compliance costs.

Option 7.3 would not allow CAs to record all fraudulent transaction cases, resulting in a lack of information for supervisory purposes.

Option 7.1 has been selected.

GL on aggregate fraud data reporting by competent authorities to the EBA and the ECB
Guideline 3: Practical data reporting

CAs could report to the EBA and the ECB the data provided by PSPs in accordance with the following options:

- Option 3.1: PSPs must send data to CAs within a specific timeline and CAs must also send the aggregate data to the EBA and the ECB within a specific timeline;
- Option 3.2: CAs must send the aggregate data to the EBA and the ECB in accordance with a general timeline, allowing MS discretion to decide the most appropriate timeline for PSPs to report to them.

Option 3.1 is not considered feasible due to differences in CAs' data reporting processes across MS. The number of PSPs that have to report data also varies across MS.

Option 3.2 addresses the issues mentioned above, allowing CAs to take into account the specificities of their market when data has to be reported to the EBA and the ECB.

Option 3.2 has been selected.

Guideline 4: Cooperation among CAs

- Option 4.1: different CAs at national level report independently to the EBA and the ECB;
- Option 4.2: different CAs coordinate and only one reports for all to the EBA and the ECB.

Option 4.1 would be easier for CAs to implement, given that it would not require any cooperation. However, the lack of coordination might lead to a lack of comparability and unnecessary complexities for the ECB and the EBA as well as the PSPs.

As a result, Option 4.2 has been selected.

D. Cost-benefit analysis

The aim of these GL is to define the set of payment transactions fraud data to be reported to comply with the requirement under Article 96(6) PSD2. The GL define fraudulent payment transactions for

the purpose of data reporting, and they set out reporting methodologies and processes to be applied, in addition to the data breakdowns to be provided. They will affect PSPs and CAs.

The expected benefits relate to the possibility of improving the effectiveness and the quality of fraud data reporting across MS. More harmonised reporting processes would allow CAs to better monitor payment fraud within the EU and the EEA and to undertake actions to address arising payment fraud issues.

In particular, improving the quality of data and its reliability and comparability will facilitate the monitoring of payment fraud and the information exchange between CAs, the ECB and the EBA, ultimately contributing to an improved level of confidence in the EEA payment services market.

Identifying and monitoring payment fraud will contribute to the better supervision and regulation of PSPs, which in turn will contribute to more effective mechanisms for fighting against payment fraud, positively affecting consumers. Consumer protection against payment fraud plays a key role in fostering the use of payment services. The future development of the EU single market will also depend on consumers' confidence and the capacity of the payment services market to facilitate the safe exchange of goods and services across Europe.

A safer and better supervised payment services market will also benefit PSPs. The use of payment services, especially innovative means of payment, across MS will depend to a great extent on ability to reduce the risk of fraud in the market.

On the other hand, the implementation of these GL will entail compliance costs for both CAs and PSPs. These costs will mainly relate to the additional reporting standards to be set out by CAs and to the increased administrative burden for PSPs.

It is reasonable to assume that most of the costs for PSPs of complying with these Guidelines will be one-off costs in order to set up new reporting and data recording processes. For CAs, it is reasonable to assume that a large part of the costs will be one-off costs to set up the process, with regular minimum ongoing costs arising from aggregating data. In addition, a number of CAs and PSPs already record fraud data, albeit using different methodologies and following different definitions. This means that the overall cost impact would be bearable, and for some Member States in particular not too significant. In addition, a number of PSPs already record fraud data for the purpose of complying either with national requirements or with industry requirements; although the data breakdowns and methodologies may differ, the overall cost impact is likely to be bearable and, in some cases, not too significant.

In conclusion, the benefits expected from better consumer protection against fraud would exceed the costs that both CAs and PSPs could face. A safer payment services market could increase the

use of payment services, creating new opportunities for all the stakeholders involved,[8] and contribute to economic growth[9].

5.2 Feedback on the public consultation and on the opinion of the BSG

The EBA publicly consulted on the draft proposal contained in this paper.

The consultation period lasted for three months and ended on 3 November 2017. The EBA also held a public hearing, which took place at the EBA's premises on 5 October 2017 and was attended by around 30 representatives of various market participants.

On 2 August 2017, the EBA published a CP, and the consultation period closed on 3 November 2017. The EBA received 48 responses to the CP, representing a wide range of market participants, predominantly trade associations, payment institutions and credit institutions. Thirty-five of these responses were published on the EBA website.

The EBA, in close cooperation with the ECB, has reviewed and assessed the responses, and has identified in the process approximately 200 different issues or requests for clarification that respondents had raised, submitting proposals to address the issues. The EBA agreed with some of these proposals, and their underlying rationale, and has made a number of changes to the GL and related annexes as a result.

In many cases, several industry bodies made similar comments or the same body repeated its comments in response to different questions. In such cases, the comments, and the EBA's analysis are included in the section of this paper where the EBA considers them most appropriate.

Changes to the draft GL have been incorporated as a result of the responses received during the public consultation.

Summary of key issues and the EBA's response

The main concerns that arose during the consultation and that resulted in the EBA making changes to the GL related to: (1) the objectives and the alignment with other instruments, (2) the categories of fraudulent transactions to be reported, (3) the scope and addressees of the GL and (4) the reporting burden (regarding frequency, date of application and detailed data breakdown).

The EBA reviewed the GL in the light of the comments received and made a number of changes, acknowledging that a number of the proposals were too burdensome with limited added value (e.g.

[8] European Commission, Green Paper on retail financial services: better products, more choice, and greater opportunities for consumers and businesses, 10 December 2015.

[9] See also: Hasan I., De Renzis T. and Schmiedel H. (2013), Retail payments and the real economy, ECB Working Paper Series No.1572.

country-by-country reporting), not sufficiently clear or accurate, or simply not relevant. In some other areas, the EBA has retained its original views and made no substantial changes.

The changes made include:

15. a change in the reporting frequency from quarterly for high-level data and annual for more detailed data to a homogenous set of data on a half-yearly basis;

16. a change in the geographical breakdown from distinguishing between three levels of geographical breakdown, including country-by-country reporting in a number of instances to a homogenous and consistent geographical reporting area for all transactions. The reporting requires a distinction between payment transactions that are domestic, cross-border within the EEA and cross-border outside the EEA;

17. a reduction in the number of categories of fraud from three to two with the exclusion of the reporting of fraudulent transactions where the payer is the fraudster;

18. a reduction in the number of data points with a focus on supervisory data;

19. the addition of specific reporting for cash withdrawals;

20. the deletion of the requirement to provide data on 'net fraud', with the PSPs required instead to report losses, independently from the transactions being reported in the same reporting period.

As stated above, a number of of the proposed requirements remain unchanged. This includes the exclusion of AISPs from the reporting obligations, the exclusion of data on prevented fraud, and the absence of a requirement to break the data down into consumer and corporate categories. The responses to all comments and queries received are included in the feedback table (pages 54 to 134).

EBA's response to the Banking Stakeholder Group's submission

The Banking Stakeholder Group (BSG) made a number of comments on the draft GL which are addressed below.

The BSG agreed with some alignment with the RTS on SCA and CSC but questioned the inclusion of all fraud categories in the calculation of the fraud rate under the RTS. They also favoured aligning fraud types in the GL with existing fraud categories in the industry. The EBA is of the view that, with the reduction from three to two fraud categories, the categories under the EBA GL are now aligned with the categories to be included for the purpose of the calculation of the fraud rate. The EBA is also of the view that an alignment with the EBA GL on incident reporting would not be achievable, given that in the latter case the reporting is event-driven and of a qualitative nature, while the fraud

Guidelines focus on quantitative information to be provided at regular interval, in line with Article 96(6) PSD2.

The BSG found the quarterly reporting excessive and favoured annual reporting, with possible more frequent ad hoc reporting. The EBA reflected on the BSG's comments and those of many other industry participants and reached the view that an appropriate and balanced frequency would be half-yearly, so that data remain relevant and up-to-date without reporting being overly burdensome.

The BSG reminded the EBA of the balance to be struck when identifying the level of data breakdown required and questioned, for instance, the need for country-by-country reporting. The EBA agreed that in some instances the level of detail would be costly, complex and not always consistent, and with only limited added value. For instance, the geographical breakdown has been harmonised to one breakdown differentiating between domestic, cross-border within the EEA and cross-border outside the EEA transactions. The revised Guidelines no longer require country-by-country data.

The BSG also suggested that the EBA limit the reporting to either the payer's PSP reporting or the payee's reporting, but not both, in order to avoid double reporting. The EBA considered the BSG's suggestion and agreed that in principle only one side of the payment chain should report. However, the EBA concluded that, for card payment transactions, both the issuer and the acquirer should report, on the basis that they would provide complementary information to the CAs, the EBA and the ECB, and concluded that acquirers should therefore also report data. The EBA has, however, clarified that in the event of the existence of acquirer and sub-acquirer, only the provider that has the relationship with the customer should report.

With regard to the exemption of AISPs, the exclusion of attempted fraud, the inclusion of net fraud and the absence of a breakdown distinguishing between consumers and corporate users, the BSG expressed diverging views, with some members agreeing with the EBA's proposals while others did not. Apart from the inclusion of net fraud, all other areas have remained as proposed in the CP. For net fraud, the EBA, after reviewing the comments received, reached the view that it would probably be unduly burdensome and would not provide regulators and supervisors with the information sought, namely the information required to enable them to form a view on losses and providers' responsibilities.

Summary of responses to the consultation and the EBA's analysis

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
General comments				
[3]	General responses	One respondent highlighted a general concern with regard to the proliferation of multiple reporting systems under different pieces of upcoming EU legislation and their impact on small PSPs.	The EBA acknowledges that a number of EU requirements require PSPs to collect and report data. Where appropriate, and in particular with regard to the relationship between the EBA GL and the ECB Regulation on payment statistics, the EBA has worked closely with the ECB to ensure that reporting requirements are aligned.	*No change*
[4]	General responses	One respondent expressed its preference for a harmonised communication method for both fraud and incident reporting in order to ensure uniformity among MS and to minimise the risk of PSPs having to develop multiple reporting mechanisms for each jurisdiction in which they are active.	The natures of, on the one hand, collecting regular statistical data and, on the other hand, reporting a major incident differ significantly. The latter is event-driven, while the former takes place at regular and recurring intervals. In addition, one relates only to quantitative data while the other one handles qualitative data as well. For these reasons, the EBA is of the opinion that the reporting mechanisms cannot be harmonised.	*No change*
[5]	General responses	One respondent suggested that national CAs should share information gathered under the GL on operational and security risks and incident reporting with market participants. This could contribute to the objectives of the fraud GL by enhancing the capacity of PSPs to manage fraud.	The EBA notes, as mentioned in the Final Report on GL on incident reporting[10], that sharing with other PSPs is not in the scope of Article 96(6) PSD2 and can therefore not be covered by the GL.	*No change*

[10] Final Report Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2), EBA/GL/2017/10, page 13

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
[6]	General responses	Some respondents requested further detail on the application of the principle of proportionality. More specifically, these respondents asked whether more information could be provided on the particular procedures, the decision-making powers and the identities of those who may apply this principle, such that a level-playing field is ensured.	The EBA is of the opinion that the principle of proportionality is included in the GL themselves, as they detail the level of information to be reported for each instrument or service. In addition, the frequency of reporting is more limited for small PIs and EMIs. The EBA does not expect any discretionary use of the proportionality principle beyond the differences that are already set out in the GL.	*No change*
[7]	General responses	One respondent noted that leaving the decision on the communication method between PSPs and CAs to CAs could result in an uneven EU playing field, i.e. PSPs could have different fraud reporting obligations depending on their location of establishment. The respondent's preference was for the EBA to align the requirements on CAs.	While the EBA acknowledges the potential downside of allowing the CAs discretion on this matter, the EBA is of the view that CAs should be able to integrate this reporting with their other regulatory reporting mechanisms. The EBA also notes that setting out procedures under the GL would prevent CAs from having the flexibility to adapt the procedures where necessary. For these reasons, the EBA is of the view that the discretion allowed the CAs on this point should be retained.	*No change*
[8]	General responses	Some respondents argued that the different schemes and/or processors (Visa, MasterCard, Amex, etc.) are already collecting data on card fraud. As a result, the respondents argued, these actors could be considered subsidiary obligated parties and could fulfil the reporting obligation for fraud involving card-based transactions for their associated PSPs.	The EBA understands the practical benefits of the proposal from the respondents. However, the EBA notes that Article 96(6) PSD2 specifically requires PSPs to collect and report data and that this responsibility cannot be delegated. In addition, a scheme approach would provide piecemeal and incomplete data, given that many PSPs are likely to use payment instruments other than cards.	*No change*
[9]	General responses	One respondent recommended that the taxonomy and terminology relating to fraud and payment instruments be aligned with the	The Directive on combating fraud considers fraud from a criminal perspective with different objectives and a different scope from the EBA GL. Given that the GL are	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		equivalents mentioned in COM (2017) proposal 489 on the EU Directive on combating fraud and falsifying means of payment other than cash, which repeals Council Framework Decision 2001/413/JHA.	drafted under Article 96(6) PSD2, they must be aligned with the terminology used in PSD2 first and foremost.	
[10]	General responses	One respondent suggested that the European Commission, the EBA and the ECB should agree on common definitions of 'fraud' to ensure that the concept is applied consistently across Europe and to provide greater clarity to supervisors and other market participants. The respondent also argued that the European Commission, the EBA and the ECB should agree on common reporting templates and practices for fraud reporting.	The EBA notes that, given that the GL are drafted under Article 96(6) PSD2, they must be aligned with the terminology used in PSD2. The EBA and the ECB have been working closely to align terminology and criteria where possible and applicable, including by aligning terminology with other relevant payment EU instruments such as the Interchange Fee Regulation (Regulation (EU) 2015/751), as referred to in the GL.	*No change*
[11]	General responses	Some respondents argued that merchants should be able to monitor and report fraud and highlighted that the current PSD2 text precludes merchants from carrying out and potentially benefiting from the SCA exemption for TRA.	It is the EBA's view that PSD2, and therefore all EBA instruments under PSD2, do not preclude merchants from having fraud detection mechanisms in place and that such mechanisms would be valuable for the protection of their customers and to prevent their own financial exposure. However, merchants are not included within the scope of PSD2 and cannot therefore be included in the EBA GL or any other instrument developed under PSD2, such as the RTS on SCA and CSC.	*No change*
[12]	General responses	Some respondents expressed the view that card schemes were better placed to identify and act on fraud trends than individual PSPs; they noted that card schemes are already covered by card payment fraud reporting and the ESCB's oversight of payment systems.	While the EBA appreciates that card schemes may have valuable information on fraud and fraud trends, the EBA also notes that PSD2 requires PSPs themselves to collect and report fraud data. In addition, the EBA is of the view that PSPs should be monitoring fraud without relying solely on schemes. The EBA also notes that the objectives of the EBA GL are primarily supervisory, by	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
			contrast with the oversight objectives of the ESCB Regulation, and, while the objectives may overlap, they will not all be the same.	
[13]	General responses	A number of respondents highlighted that PSPs are already obliged to report most of the required statistical information on the volumes and values of the different types of payment transactions they process, due the reporting obligations set out in the ECB Regulation on payment statistics (Regulation (EU) No 1409/2013 of the ECB of 28 November 2013 on payments statistics (ECB/2013/43)). This implies an overlap in the data to be reported by PSPs. Respondents therefore suggested that the GL should refer to the ECB Regulation on payment statistics. Those respondents also noted that the ECB Regulation was to be revised.	The EBA is aware of the potential overlap of the EBA GL with the ECB Regulation on payment statistics with respect to reporting payment transactions by payment service/instrument. Therefore, the EBA has been working in close cooperation with the ECB to ensure that the data required by the two entities are aligned. When finalising the EBA GL, the EBA and the ECB have also taken into account the feedback provided by PSPs in the context of the fact-finding conducted by the ESCB with respect to the potential revision of the ECB Regulation on payment statistics. In addition, please also see our response to comment [12].	*No change*
[14]	General responses	A number of respondents expressed the view that the data under the ECB Regulation on payment statistics and under the EBA GL should be reported only once to CAs and that duplication of reports should be avoided.	The EBA agrees that the risk of double reporting should be minimised, wherever possible. The EBA notes that the obligation to report to the ECB and the EBA in PSD2 lies with the CAs rather than the PSPs. The EBA also notes that the CAs recognised as competent under PSD2 may differ from the reporting authorities for the purpose of the ECB Regulation on payment statistics. Where appropriate, national authorities designated as competent under PSD2 and those designated as competent under other legislation on statistical reporting may decide at their discretion to collect data only once as suggested in the comment. This is not, however, within the scope of these GL.	No change

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
[15]	General responses	One respondent noted that it was unclear how actual fraud cases should be mapped in alignment with the data breakdowns and which parties were actually required to report the fraud.	The EBA acknowledges that this may not always have been clear in the draft and has made some changes in a number of areas, as described in sections 3.2 and 4 (GL themselves) of the Final Report, for example to Guideline 1, including by linking Guideline 1.6(c) and 1.6(d) to Guideline 1.1(a); changes have also been made to the different breakdowns in Annex 2. On the question of which parties are actually required to report the fraud, the EBA clarifies that as a general rule for all types of payment services, the payer's PSP has to report, except for direct debit transactions, which are reported by the payee's PSP. In addition, card payments are reported both by the payer's PSP (the issuer) and the payee's PSP (the acquirer). In addition, Guideline 1.2 clarifies that only transactions that have been initiated and executed should be reported, meaning, inter alia, that 'simple book entry'-type transactions should not be taken into account, since they have been executed without a specific transaction order, i.e. without the use of a payment service.	Guideline 1.6.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; Guideline 1.6.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's/payee's sensitive payment data through fraudulent means.
[16]	General responses	One respondent expressed the view that high-level, infrequent reporting requirements would not add value, given that PSPs are already incentivised to fight fraud (for the benefit of their customers and merchants). Furthermore, these respondents added that	The EBA notes that the reporting of fraud statistics is a requirement under Article 96(6) PSD2. The EBA does not agree with the comment that the fraud reporting will not add any value, as it will provide both supervisors and PSPs with relevant insights into fraud patterns and fraud affecting particular payment instruments. Nonetheless, the EBA agrees that a balance has to be found with regard to the frequency of reporting.	GL 3.1 and 3.2 have been changed as follows: 3.1 The payment service provider should report data ~~on~~ **every six months based on the applicable data breakdown(s) in Annex** 2 a~~n annual basis based on the applicable data breakdown(s) in Annex 2, and data, on a quarterly basis, based on~~

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		these reporting requirements would only create an additional burden for PSPs.	Therefore, the EBA has altered the proposed quarterly reporting to half-yearly reporting and annual reporting for small PSPs.	~~the applicable data breakdown(s) in Annex 3, depending on the service provided and the payment(s) instrument(s) used~~. 3.2 The payment service provider that ~~may~~ benefit**s** from an exemption under Article 32 PSD2 and e-money institutions that may benefit from the exemption under Article 9 of Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions (EMD) should report the ~~full~~ set of data required in the applicable form(s) **in** ~~under~~ Annex ~~1~~**2 only** on an annual basis. Annex 3 has been deleted and the references to 'quarterly' in Guideline 7 and GL 2.8, 3.1, 9.6 and 10.4 have been deleted.
Feedback on responses to question 1				
[18]	GL' objectives	One respondent was of the opinion that the objective of the CAs, and ultimately the EBA, should be not only to gather information on fraud but also to enhance the strategies of PSPs to manage fraud.	The EBA is of the view that collecting and reporting fraud data in compliance with the GL will contribute to the capacity of PSPs to identify fraud. However, it remains the responsibility of PSPs, not of public authorities, to develop strategies to manage fraud.	*No change*
[19]	GL' objectives	One respondent proposed that an additional objective should be added with the aim of encouraging PSPs to use the fraud reporting under the Guidelines to optimise their use of TRA.	The EBA is of the view that the GL will enable PSPs to have high-level information on the usage of any of the exemptions provided for under the RTS on SCA and CSC.	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
[20]	GL' objectives	One respondent was of the view that statistical data could only provide information on long-term trends rather than specific fraud scenarios and would not help to enhance understanding of changes in fraud patterns on a continuous basis (or in the short term). In the respondent's view, the required data may help only in assessing the general effectiveness of what PSD2 is intended to achieve (i.e. the level of overall security).	The EBA is of the view that real-time continuous fraud monitoring is for PSPs to undertake. The data required by the GL will provide information on yearly and half-yearly trends. It will enhance understanding of changes in fraud patterns over these periods and help in identifying potential issues specific to firms and specific to particular means of payment.	*No change*
[21]	GL' objectives	A number of respondents questioned the link made with the RTS on SCA and CSC and suggested removing the link with the fraud rate calculation and with the monitoring of the use of the TRA exemption. They argued that CAs can access other data, such as annual audit reports, in relation to the RTS on SCA and CSC.	The EBA does not agree that the link to the fraud rate calculation should be completely removed given that supervisory authorities need to have a view on the fraud levels related to the payment services provided. The GL are a tool for these authorities to monitor compliance with PSD2 itself and the technical standards and GL that the EBA has developed in support of the Directive, including the RTS on SCA and CSC. This link is important and we have clarified it in section 3.2 of the Final Report.	*Reference to the RTS on SCA and CSC in section 3.2 of the report, paragraph 12*
[22]	GL' objectives	One respondent encouraged the EBA to include further detail in the GL to ensure accurate and consistent reporting, arguing that the GL as currently drafted (with regard to both the annual and the quarterly reports) do not give the level of granularity required.	The EBA is of the view that not all possible detail can or should be included in the GL, given that the EBA has to strike an appropriate balance between the competing demands of obtaining accurate data and ensuring a proportionate compliance burden for firms. The EBA therefore disagrees with the view that further detail should be included.	*No change*
[23]	GL' objectives	While a number of respondents expressed reservations, a large number of respondents supported the publication of aggregate data, mostly on the basis that it could be a useful	The EBA agrees with the respondents that data should only ever be published in an anonymised form and on a confidential basis. The EBA has therefore emphasised	*Paragraph 15 of section 3.2 of the report clarifies that any publication would be of anonymised aggregate data*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		tool for PSPs to benchmark themselves against. A number of respondents, however, queried whether the data published would provide specific information on providers and suggested explicitly stating in the objectives that the statistics made available to the authorities by the PSPs should be treated as confidential and anonymised if/when published. Some respondents also asked that the EBA consult prior to publication with the industry and the ECB on common quality and reporting standards. Some respondents also suggested that reports should be published only once the measures are reliably set up in each Member State.	this anonymity in section 3.2 of the Final Report. The decision on whether or not to publish any data by CAs, the EBA or the ECB would be a decision independent of these GL; it has not been made yet, and no publication is currently envisaged.	
[24]	GL' objectives	A number of respondents stated that setting up the exchange of fraudulent data (such as ID documents, names, IBANs, phone numbers or other information used for committing fraud) between PSPs, ideally via CAs, should be an objective.	Information exchange between PSPs is not within the scope of the mandate conferred on the EBA in Article 96(6) PSD2, which refers only to reporting from PSPs to the EBA and the ECB. No objective of the kind suggested by the respondent can therefore be added.	*No change*
[25]	GL' objectives	One respondent was of the opinion that the objectives should include automated reporting to law enforcement authorities for information purposes.	The EBA is of the view that given the statistical and quantitative nature of the reporting, it is unclear what an automatic link to law enforcement would achieve (or, furthermore, how it could be achieved). Information exchange between the EBA and other EU authorities is not within the scope of the mandate conferred on the EBA in Article 96(6) PSD2, which refers only to reporting	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
			from PSPs to the EBA and the ECB. No objective of the kind suggested by the respondent can therefore be added. By way of comparison, the EBA would like to refer to the separate mandate conferred on the EBA in PSD2 to develop GL on major incident reporting under PSD2 (EBA/GL/2017/10). Here the EU legislators did include in the scope of the mandate a requirement for the EBA and the ECB to share the reports received with other relevant EU authorities, and this is reflected accordingly in the GL.	
[26]	GL' objectives	One respondent suggested that the objectives should take into account the needs of other European authorities and that the EBA should be clear on how data will be shared across the EEA, what institutions will have access to the data (including EU institutions), in what manner and on what terms.	As expressed in more detail in response to comment [25], Article 96(6) PSD2 specifically requires PSPs to provide data to CAs and for these authorities to provide aggregated data to the EBA and the ECB. There is no mention of further EU authorities and, for this reason, the EBA does not wish to add such an objective.	*No change*
[27]	GL' objectives	A number of respondents argued that a harmonised application of requirements across all MS was essential to ensure consistent compliance with the GL and that therefore, this should be explicitly added to the objectives of the GL.	Convergence and harmonisation is the primary objective of the GL and of the EBA more generally. The EBA Regulation specifies the legal standing of GL, including the comply-or-explain procedure and that financial institutions have to make every effort to comply with GL. The EBA therefore sees no need to add an additional objective in this regard.	*No change*
[28]	GL' objectives	A number of respondents expressed the view that the design of the fraud reporting requirements should be aligned with the calculation of fraud rates and monitoring articles under the RTS on SCA and CSC and any other relevant EBA GL.	The EBA is of the view that the EBA GL should specify a broad set of data with the required breakdown to provide some read-across with other EBA instruments. Where applicable, the terminology used should be aligned. The EBA would also like to clarify that the same two categories included in the reporting for the purpose	*Clarification in paragraph 12 of section 3.2 of the report*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
			of the EBA Guidelines, namely unauthorised transactions and transactions as a result of the manipulation of the payer, should be used to calculate the fraud rate under Article 18 of the RTS on SCA and CSC, as mentioned in paragraph 46 of the EBA Opinion on the implementation of the RTS on SCA and CSC. The EBA has amended section 3.2 of the Final Report to clarify this.	
[29]	GL' objectives	One respondent highlighted the contradiction between the objective 'to proactively identify fraud trends for future risk identification and proactive mitigation' and the Guidelines being a supervisory tool used to understand whether there are market-wide or PSP-specific issues related to fraud, with the former requiring day-to-day monitoring while the latter requires annual reporting.	The EBA is of the view that the statements are not contradictory. While the GL will not enable day-to-day monitoring of fraud trends, the data obtained will enable CAs to identify fraud trends as they emerge over the collection periods and take necessary action. Day-to-day monitoring remains the responsibility of firms. The EBA is of the view that it has reached an appropriate balance between competing demands, by requiring half-yearly reporting of data broken down by quarter to enable the identification of trends intra-year, which can then be acted on by CAs.	*No change*
[30]	GL' objectives	One respondent was of the view that the objectives lacked a description of the scope of Article 96(6) PSD2, particularly clarification on whether PSD2 calls for statistical data for macroprudential oversight of payment markets or microprudential supervision of individual PSPs.	The EBA is of the view that the data are for both macro and micro purposes, given the variety of roles of the EBA and the ECB, ranging from supervision of PSPs to market monitoring and oversight of payment systems.	*No change*
[31]	GL' objectives	One respondent expressed the view that the EBA had no mandate to collect payment statistics to enhance the oversight of the ESCB of payment systems.	Article 96(6) PSD2 provides that fraud statistics data on means of payments have to be reported to both the ECB and the EBA. These GL are aimed at CAs, who are to provide data to both the EBA and the ECB, but they focus on data mostly relevant for regulatory and supervisory	*Changes include the deletion of country-by-country data with the introduction of a new homogenous geographical area highlighted in Guideline 4.1 and Annex 1.*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
			functions. The EBA, in close cooperation with the ECB, has concluded that the Guidelines do not cover needs that are exclusive to overseers of payment systems and instruments. More detailed data for the exclusive purpose of oversight of payment systems and instruments may be further required by the ECB by means of other legal instruments. The EBA is of the view that Article 96(6) PSD2 provides such a mandate, given that these Guidelines are aimed at CAs, who are to provide data to both the EBA and the ECB. Following the assessment of the consultation responses, the ECB and the EBA agreed that the more detailed and granular data required for oversight purposes would be best covered in the separate and pending ECB Regulations, and that the EBA Guidelines should stay at a higher level. Changes have therefore been made to the final Guidelines.	Guideline 4.1: Payment service providers should report data for transactions that are domestic, cross border within the EEA, and cross-border ~~one-leg~~ outside the EEA ~~by breaking the transactions down per country for EEA countries, and as an aggregate for non-EEA countries~~. Annex 1: ~~Geographical~~ Area ~~1~~: **Domestic; Cross-border within the EEA; and** Cross-border **outside the EEA**
[32]	GL' objectives	A number of respondents expressed concern about the fact that one of the objectives is to assist PSPs with the monitoring of compliance with the requirements of the RTS on SCA and CSC, as these draft GL are linked to Articles 18 and 20 of the draft RTS. While such an alignment of definitions and approaches is generally welcomed and may be helpful for PSPs in theory, it is not clear how this would work in practical terms. The respondents were of the view that the proposed linking of the two issues might, in practice, add an unwelcome element of complexity to what should be a standard regulatory reporting exercise.	The EBA has reflected on the question of the relationship with the RTS on SCA and CSC and agrees that a direct link for PSPs with the RTS as an objective might have unintended consequences, as practical considerations may vary. The EBA is, however, of the view that such a link should remain for CAs as well as the EBA. Indeed, the Guidelines aim to contribute to CAs' supervision of PSPs' application of, and compliance with, the RTS for CAs. The GL also aim to contribute to providing information on the use of exemptions and the application of SCA in the context of the EBA review of the RTS, scheduled for 18 months after its date of application. In addition, the categories of transactions to be taken into account for the purpose of calculating the fraud rate are the same as those defined in Guideline 1 and mentioned in paragraph 46 of the EBA Opinion on the implementation of the RTS	*Clarification provided in paragraph 12 of section 3.2.*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
			on SCA and CSC. Both are specified in paragraph 12 of section 3.2 of the Final Report. See also comments [21] and [28]	
[33]	GL' objectives	One respondent argued that if the Guidelines were for informational and statistical purposes, the required information would be far too detailed. The respondent also stated that if the objectives of the Guidelines were to contribute to improving the strategies of PSPs for handling fraud, the proposed data breakdown could be considered appropriate.	The EBA is of the view that these GL have two objectives: (i) to provide statistical information to supervisors and (ii) to enhance the awareness of PSPs and help them improve their strategies for handling fraud. In order to find a more proportionate balance between these two objectives, the EBA has reviewed the data breakdown required in Annex 2 and Guideline 7.	*Guideline 7:* Data breakdown 7.1 For **e-money payment transactions** ~~e-money transactions~~ as defined in Directive 2009/110/EC, the payment service provider should provide data in accordance with Data Breakdown **FA** in Annex 2 ~~and Data Breakdown E in Annex 3~~. 7.2 When providing data on e-money **payment** transactions, the payment service provider should cover e-money ~~account~~ payment transactions a. where the payer's PSP is identical to that of the payee; and b. where a card with an e-money function**ality** is used. 7.3 The payment service provider for the purpose of **e-money payment transactions** ~~e-money transactions~~ should report data on volumes and values of all payment transactions, as well as volumes and values of fraudulent payment transactions ~~(net and gross)~~, with the following breakdowns: a. geographical perspective, b. payment channel, c. authentication method, d. reason for authentication choice (referring to the exemptions to strong customer authentication detailed **in** ~~under~~ Chapter 3 of the Regulatory

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
				Technical Standards on Strong customer authentication and common and secure communication, **Commission Delegated Regulation (EU) 2018/389** ~~EBA/RTS/2017-02~~), and e. fraud types. ~~For the purpose of quarterly reporting, the payment service provider executing e-money transactions is not required to report the data specified in points (d) and (e) of Guideline 7.3 nor data on net fraudulent payment transactions.~~ 7.4 For money remittance services, the payment service provider should provide data in accordance with Data Breakdown **GB** in Annex 2 ~~and Data Breakdown F in Annex 3~~ **and as specified** in ~~line with the~~ 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 ~~(net and gross)~~ in ~~line with~~ Guideline 2.1 and with **the** geographical ~~breakdown~~ **perspective**. 7.5 When providing payment initiation services, the payment service provider should provide data in accordance with Data Breakdown **GC** in Annex 2 ~~and G in Annex 3~~. The payment service provider should report the executed payment transactions it initiated and the executed fraudulent transactions ~~(net and gross)~~ it initiated, both in volume and value.

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
				7.6 For those payment transactions that qualify under Data Breakdown **G** ~~C~~ in Annex 2 ~~and G in Annex 3~~, **the payment service provider** ~~PSPs~~ 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. ~~For the purpose of quarterly reporting, the payment service provider offering payment initiation services is not required to provide data under point (b) of Guideline 7.7.~~ **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 both in volumes and values, in accordance with Data Breakdown C and/or E in Annex 2. When such data are provided, the provider should ensure that no double-reporting occurs.** 7.8 The payment service provider offering credit transfer and card **based** payment ~~based~~ services should provide data **in accordance with** ~~included in~~ Data Breakdowns **A, C and D** ~~D1, D3 and D4~~ in Annex 2 ~~and Data Breakdown H1, H3 and H4 in Annex 3~~, depending on the payment

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
				instrument used for a given payment transaction as well as the role of the payment service provider. The data include: a. geographical ~~breakdown~~ **perspective**, b. payment channel, c. authentication method, d. reason for authentication (referring to exemptions to strong customer authentication detailed under 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 D**. ~~For the purpose of quarterly reporting the payment service provider is not required to provide the data listed under points c), d) and e).~~ 7.9 The payment service provider should provide data **in accordance with** ~~included in~~ Data Breakdown **A**~~D1~~ in Annex 2 ~~for annual reporting and Data Breakdown H1 in Annex 3 for quarterly reporting~~ 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 C in Annex 2 for all payment transactions and fraudulent payment**

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
				transactions executed using direct debits. The data include: **a. geographical perspective,** **b. channel through which consent was given, and** **c. fraud types.** 7.11 The payment service provider should provide data ~~included in~~ **in accordance with** Data Breakdown **C** ~~D3~~ in Annex 2 ~~for annual reporting and Data Breakdown H3 in Annex 3 for quarterly reporting~~ for all ~~the~~ payment transactions on the ~~sending~~ **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 ~~included~~ in **accordance with** Data Breakdown D~~4~~ in Annex 2 ~~for annual reporting and Data Breakdown H4 in Annex 3 for quarterly reporting~~ for all payment transactions on the ~~receiving~~ **acquiring** side where a **payment** card was used and the payment service provider ~~is~~ **was** the payee's payment service provider. **7.13 The payment service provider providing data in accordance with Data Breakdown A to D and Data Breakdown F in Annex 2 should report all losses due to fraud per liability bearer during the reporting period.** ~~The payment services provider PSP should provide data in Data Breakdown D2 in Annex 2 for annual reporting and Data~~

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
				~~Breakdown H2 in Annex 3 for quarterly reporting for all payment transactions and fraudulent payment transactions executed using direct debits. Data included are less detailed than for credit transfers and card based payment based services.~~ **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 payer's payment service provider (issuer) should provide data included in Data Breakdown E in Annex 2 for all cash withdrawals and fraudulent cash withdrawals through apps, at ATMs, at bank counters and retailers ('cash back') using a card.**
Feedback on responses to question 2				
[34]	Clarity on the link between fraudulent categories and the breakdown by fraud types	A number of respondents were of the view that further clarity on the link between the fraudulent payment transactions that have to be reported under these GL, as defined in GL 1.1 and 8.1, and the fraud types that are required in different sections of Annex 2 should be provided (e.g. four types are listed under section A, Table 5). Some respondents also argued that further clarity with regard to the link between GL 1.1 and 1.6(i) and (ii) should also be provided.	The EBA agrees that the link could have been clearer. Therefore, a number of changes were made as a result to Guideline 1.6 and Annex 2.	Guideline 1.6: 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

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
				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's/payee's sensitive payment data through fraudulent means.
[35]	Scope and definition of the GL	With reference to the TRA and the reason for authentication choice reporting, some respondents queried whether it was possible to separate out the payment instruments for the TRA calculation (e.g. private cards versus bank cards, digital wallet versus card) to enable the exemption from SCA to apply depending on the payment instrument.	The EBA is of the view that any further breakdown on authentication would not be proportionate and would result in the GL creating an excessive burden. The EBA also notes that the RTS on SCA and CSC do not require any such breakdown and distinguish only between credit transfers and card payment transactions.	*No change*
[36]	Scope of the GL	One respondent queried whether a fraud when opening a payment instrument ('false customer') was within the scope of GL on fraud reporting or whether they covered only fraud when a 'real' customer contested a payment transaction.	The GL cover payment transactions that are fraudulent that were unauthorised or the result of the manipulation of the payer. The GL do not cover the setting up of a payment account. Furthermore, the GL do not require reporting on cases where the payer is the fraudster.	*No change*
[37]	Scope of the GL	One respondent queried the categorisation of revolving cash reserve dissociated from a card.	The EBA agrees that further clarity was needed with regard to the fraud types included in Annex 2. The EBA has made a number of changes to clearly align those types with the definition; it is an ancillary service to the	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
			provision of payment services and therefore need not be reported.	
[38]	Scope of the GL	Another respondent queried whether credit repayments and money recovery were within the scope of the GL.	The GL cover all payment transactions that have been executed and/or acquired (whether or not they have been initiated by a different PSP). The EBA is therefore of the view that credit repayments and money recovery are within the scope of the GL and are to be included providing payment transactions were executed to carry out those repayments and recovery. Similarly, payment transactions executed to refund a customer are included.	*No change*
[39]	Clarifying fraud types	One respondent suggested clarifying the fraud types to be reported in relation to the definition of 'fraudulent payment transaction'.	The EBA agrees that further clarity was needed with regard to the fraud types included in Annex 2. The EBA has made a number of changes to clearly align those types to the categories provided in Guideline 1.1. See also comment [34]	*Guideline 1.6(h) on manipulation of the payer has been deleted and former Guideline 1.1(c) (now 1.1.(b)) has been redrafted as follows:* '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')**.' *Changes to the sub-categories of fraud type in Annex 2, Data breakdowns A to D and F.*
[40]	Clarity of definitions	One respondent argued that many areas of the GL were open to different interpretations, encouraging the EBA to provide greater clarity on definitions for each of the data elements being sought, as well as further guidance on reporting.	With regard to the terminology that is used and defined in PSD2, the GL cannot legally provide any further clarification, and therefore no changes were made. With regard to other terminology, the EBA agrees that some terminology used needed to be clearer, in particular with regard to the definition of 'fraud'. As a result, the definition of 'manipulation of the payer' has been refined	*Guideline 1.6(h) on manipulation of the payer has been deleted and former Guideline 1.1(c) (now 1.1.(b)) has been redrafted as follows:* '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,**

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
			in Guideline 1.1(b) and Guideline 1.6(h) has been deleted.	**to a payment account it believes belongs to a legitimate payee ('manipulation of the payer')'**.
[41]	The inclusion of the categories of 'payer being the fraudster' and 'fraudulent transaction due to the manipulation of the payer'	A number of respondents were of the view that the focus of the GL should be on unauthorised transactions only. In the view of these respondents, for the purposes of fraud reporting within the scope of PSD2, the inclusion of transactions carried out by the genuine account holder acting fraudulently or being manipulated would distort any assessment of the effectiveness of using SCA. For example, they argued that where the payer/genuine account holder has acted fraudulently, otherwise known as first party fraud, this would not demonstrate the effectiveness of the customer authentication method undertaken by the PSP. Respondents argued that the same principle applied to the manipulation of the payer, commonly recorded in the UK as APP (authorised push payments). Reasons for excluding these types of fraud included: • The manipulation targets only the payer as an individual person; the payment transaction itself is not affected, so such fraudulent actions (fraudulent actions prior to payments) do not fall within the	As stated in the CP, the EBA is of the view that recording all types of fraud is very important in order to be able to identify whether the types of fraud used evolve, but also to be able to identify the efficiency of regulatory intervention (e.g. the requirement to use SCA) for each type of fraud. That being said, the EBA has reflected on the comments and has reached the view that fraud where the payer was the fraudster (also known as first party fraud) should not be included, on the basis that it does not reflect on the effectiveness of payment systems. The EBA, however, remains of the view that manipulation of the payer is a relevant category for assessing such effectiveness. Indeed, such fraud cases are caused by a third party manipulating a payer into making a payment and it is, at least partially, the responsibility of the PSP to identify such cases. This is particularly the case with regard to the use of transaction monitoring systems, and in particular TRA. This is of particular concern to the EBA given that this type of fraud has significantly increased. The EBA acknowledges that the data for the two categories of fraud listed in Guidelines 1.1(a) and 1.1(b) may not be equally reliable and comparable at the outset and that it may take time for the data set on manipulation of the payer to mature.	*Guideline 1.6(h) has been deleted* ~~payment transactions made and authorised by the payer that acted dishonestly or by misrepresentation, whether or not with intent to make a gain for himself or another, and that denies having authorised the payment transaction;~~ *Former Guideline 1.1(c) (now 1.1.(b)) has been redrafted as follows:* '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')**.' *Changes to the sub-categories of fraud type in Annex 2, Data breakdowns A to D and F.*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		scope of PSD2, and the transactions will in fact have been executed correctly. • It would be impossible for PSPs to prevent those fraud activities by means of SCA or by authentication means with even higher security standards. • PSPs do not have information on those types of fraud and would not be able to provide data. It is very difficult to identify where the exact origin of social engineering is. Although they are morally and ethically questionable, counting these transactions as fraudulent would increase the fraud rate associated with a payment service. • Identification of social engineering-based frauds often takes place a considerable time after the fraud has taken place, and these frauds may therefore be underreported as a result. • The burden imposed on PSPs seems disproportionate. So-called 'CEO fraud', for example, is in the respondents' opinion not payment fraud, but a fraud scheme using social engineering, similar to fraud types such as the so-called 'grandchild fraud'. • Such transactions are not covered by Article 96(6) PSD2.		

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		If the EBA keeps the payer manipulation category, one of the respondents suggested that it clarify that this refers only to manipulation of systems or mechanisms applied or controlled by a PSP.		
[42]	Scope of the GL	A number of respondents specifically suggested that the definition in the GL exclude (operational) errors.	The EBA agrees with the respondent and would like to highlight that operational errors are not covered by the GL. However, the EBA is not of the view that this needs to be explicitly reflected in the definition.	*No change*
[43]	Scope of the GL	One respondent was of the view that fraud reporting would be more meaningful if the data collection was based on the correlation between the fraudulent event, the payment instrument and the specific channel used.	The EBA notes that the breakdown of data includes fraud types and also cross-referencing distinguishing between remote and non-remote transactions. In addition, the EBA notes that the GL specify different breakdowns depending on the instrument used. The EBA is therefore of the view that such correlations are made to the extent possible.	*No change*
[44]	Scope of the GL	One respondent queried whether mule accounts were within the scope of the GL or not.	The GL include all executed fraudulent payment transactions. If payment transactions from a mule account are fraudulent in accordance with the definition provided in Guideline 1.1, these transactions should be included in the reporting.	*No change*
[45]	Definition of delayed debit cards	One respondent queried the definition of a 'delayed debit card'.	'Delayed debit card' in the EBA GL has the same meaning as in the ECB Regulation on payment statistics, namely 'a card enabling cardholders to have their purchases charged to an account with the card issuer, up to an authorised limit with the balance on the account settled in full at the end of a pre-defined period'. This is commonly referred to as a 'charge card'.	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
[46]	Definition of fraud	One respondent suggested that the EBA review the definitions of 'fraud' provided in Guideline 1 to ensure that they are complete and encompass all fraud types on which PSPs must report.	In Guideline 1.1, the EBA identifies two categories of fraudulent transactions. The EBA cross-referenced existing fraud types used in the industry and on that basis identified a number of sub-categories within the category of unauthorised transactions, detailed in the data breakdown in Annex 2.	*Guideline 1.6(h) has been deleted* ~~payment transactions made and authorised by the payer that acted dishonestly or by misrepresentation, whether or not with intent to make a gain for himself or another, and that denies having authorised the payment transaction;~~ *Former Guideline 1.1(c) (now 1.1.(b)) has been redrafted as follows:* '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')**.' *Changes to the sub-categories of fraud type in Annex 2, Data breakdowns A to D and F*
[47]	Fraud rate under the RTS on SCA and CSC	A number of respondents argued that counting other transactions in addition to unauthorised transactions as fraudulent would increase the fraud rate associated with a payment service and hinder the PSP's ability to exempt certain transactions from SCA, even though the so-called 'fraudulent transaction' had been subject to SCA.	The Guidelines include two categories of fraudulent payment transactions. While these categories are defined for the purpose of the Guidelines, there is a link with the RTS on SCA and CSC, as detailed in paragraph 12 of section 3.2 of the Final Report. See also comments [21], [28] and [32]. The EBA adds that, given the wording 'unauthorised or fraudulent' in PSD2 and the RTS on SCA and CSC, the EBA is of the view that the calculation should include both categories of fraud, as explained in paragraph 46 of the	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
			EBA Opinion on the implementation of the RTS on SCA and CSC.	
[48]	Geographical scope of the GL	One respondent argued that transactions where the payee is resident outside the EEA or where the POS is deployed outside the EEA are 'one-leg-out' transactions and that such cases should be reflected in the definitions.	The EBA notes that one-leg-out transactions are included in transactions outside the EEA, as defined in Guideline 1.1(f) (former Guideline 1.1(e)). The EBA agrees that the distinction regarding geographical area was not clear. Therefore, the requirements regarding the geographical area and the corresponding Guideline 4.1 have been refined to clearly distinguish between one-leg-out transactions, cross-border transactions within the EEA and domestic transactions as defined in Annex 1.	*Guideline 4.1:* Payment service providers should report data for transactions that are domestic, cross border within the EEA, and cross-border ~~one-leg-~~outside EEA ~~by breaking the transactions down per country for EEA countries, and as an aggregate for non-EEA countries~~. *Annex 1:* ~~Geographical~~ Area ~~1~~: **Domestic; Cross-border within the EEA; and** Cross-border **outside the EEA**
[49]	Definition	One respondent asked the EBA to further clarify what is meant by 'executed' in the context of a transaction.	The term 'executed' should be understood in the sense of PSD2, i.e. when the account servicing payment service provider (ASPSP) has processed (or acquired) the payment transaction and the funds have been transferred to the payee's PSP. Guideline 1.2 now includes a reference to acquiring also.	*Guideline 1.2:* For the purposes of **Guideline** ~~paragraph~~ 1.1 above, the payment service provider **(including the payment issuer where applicable)** should report only payment transactions that have been initiated and executed **(including acquired where applicable)**
[50]	Definition	One respondent requested a more detailed description of fraud where the payer has acted fraudulently.	As stated in the response to comment [41], this category is no longer to be reported under the Guidelines.	*Guideline 1.1.b deleted*
[51]	Fraud types	Some respondents considered that, given that fraud was dynamic, adding an 'other'	The EBA has reflected on these suggestions and has decided not to include an 'other' category on the basis	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		category to the fraud types in Annex 2 would be appropriate. Other respondents preferred the adoption of a broad approach to the categories to ensure that all future forms of fraudulent payment transactions would be included in the reporting.	that adding such a category would lead to a risk of skewing the data and making the statistics less understandable. The EBA agreed with those respondents who favoured a broader approach to the definition of the categories of fraud types.	
[52]	Scope	One respondent was of the view that the GL should clarify the link and connection with sensitive payment data under PSD2.	The EBA notes that 'sensitive payment data' is defined by PSD2 and cannot be further clarified in the GL. In addition, rather than focusing on qualitative data, the GL focus on payment transactions and related quantitative data.	*No change*
[53]	Definition and fraud types	Some respondents suggested customising the definitions and breakdown of types of fraud for each payment instrument.	The EBA considered these comments and reached the view that for the purpose of ensuring the consistency and transparency of the GL, they should include general categories regardless of the instrument or type of service. However, the EBA agrees that the link between these two categories and the sub-categories of named fraud types in Annex 2 was not always clear. The EBA has, as a result, refined and updated these fraud types. The fraud types are specific to each payment instrument.	*Changes to the fraud type sub-categories in Annex 2, Data breakdowns A to D and F*
[54]	Scope and definition	One respondent encouraged the EBA to clarify in the fraud-type section that any disputes between payer and payee with respect to the underlying business transaction should not be considered fraud or fraudulent transaction.	The EBA agrees that a dispute is not synonymous with fraud but is not of the view that this specifically needs to be reflected in the categories of fraud defined in Guideline 1.1.	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
[55]	Scope and relation with the RTS on SCA and CSC	Some respondents argued that the only reasonable definition of 'fraudulent payment transactions' to be counted to calculate the fraud levels for the TRA exemption were those related to the security features of the means of payment and, specifically, those situations in which the legitimate payer did not authorise the execution of payment. These are defined in PSD2 (Article 74) as 'unauthorised payment transactions' where the payments result from the 'loss, theft or misappropriation of a payment instrument'. Irrespective of whether the EBA decides to maintain a broader definition of 'fraudulent payment transaction' for reporting purposes, it should be clarified that this definition does not apply for the purposes of Articles 18 and 20 of the RTS on SCA and CSC (i.e. for the calculation of ETV fraud thresholds for TRA).	The EBA disagrees that only unauthorised transactions relate to the security features of the means of payment and indeed is of the view that manipulation of the payer also relates to those features. The EBA, however, agrees that the payer being the fraudster himself would be of a different nature and this type of fraud has therefore been excluded. See the response to comment [41].	*See the response to comment [41] in reference to the deletion of former Guideline 1.1.b*
[56]	Definition	A number of respondents asked the EBA to clarify the definition of 'manipulation of the payer' to ensure that data are comparable. Some suggested including specific examples or user stories to further mitigate that risk. One respondent specifically suggested that the definition could have three characteristics: (a) the payer instructs payment in good faith at the time of payment; (b) at the time of payment, the payer confirms the payment destination; and (c) (possibly) the fraudster	The EBA has provided some clarification of the definition but is not of the view that further detail should be provided. See also comment [41].	*See the response to comment [41] in reference to the deletion of former Guideline 1.1(b)* *Guideline 1.6(h) on manipulation of the payer has been deleted and former Guideline 1.1(c) (now 1.1.b) has been redrafted as follows:* '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')**.'

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		impersonates a payee or the payee himself is fraudulent.		
[57]	Fraud categories	One respondent was of the view that an additional category for payee fraud should be added (i.e. merchant fraud, where, for example, a seller (payee) may advertise goods at an attractively low price without actually having any such goods or any intention to deliver them). These sorts of frauds, which originate with the payee, tend to occur less frequently than attacks on the payer's accounts, but can be significant in terms of financial impact, and deserve their own category.	As highlighted in the response to comment [41], the EBA has reached the view that cases where the payer himself is fraudulent (also known as first party fraud) should be excluded from the reporting, on the basis that such fraud does not reflect on the effectiveness of payment systems. In a consistent manner, the EBA is of the view that fraud on the part of the payee should also be excluded, unless the fraud has occurred through the use of a means of payment.	*No change*
[58]	Practical specificati ons	More detailed definitions are needed for various terms that are used, for example 'Transactions initiated electronically', 'remote card-based payments', 'MOTO', 'paper based'.	The EBA notes that the terms 'MOTO' and 'paper-based' have been removed from the Guidelines, on the basis that the breakdown of non-electronic payment transactions was not relevant for the purpose of this statistical data collection and reporting, as the scope of PSD2 is limited to electronic payment transactions. The EBA is unable to define 'Transactions initiated electronically' or 'remote card-based payments' because they are defined by PSD2 itself.	*The sub-categories of MOTO and paper-based payments under non-electronic payment transactions have been removed from Annex 2*
[59]	Scope and relation with the RTS on SCA and CSC	One respondent argued that the fraud rate definition should be left to the PSP in accordance with Article 17 of the final draft RTS on SCA and CSC, whereas implicitly the fraud rate is defined by this CP.	The EBA disagrees and is of the view that PSD2 refers to 'unauthorised or fraudulent' transactions and that this is term is linked to the scope of the Guidelines and includes both unauthorised transactions and manipulation of the payer, as explained in paragraph 12 of section 3.2 of the Final Report. See the responses to comments [47] and [55].	*Clarification provided in section 3.2 of the report, paragraph 12*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
[60]	Fraud types	A number of respondents suggested that the fraud types should be aligned with those used internationally by the industry. These respondents pointed out that actual fraud-type codes used by payment schemes are: Lost/Stolen Never Received Issue Fraudulent Application Counterfeit Card Fraud Account Takeover Fraud Card Not Present Fraud Multiple Imprint Fraud Bust-out Collusive Merchant	The EBA is of the view that the sub-categories (fraud types) in the data breakdown are, wherever possible and to the extent compatible with PSD2, aligned with the terminology and main categories used by the industry. Nevertheless, the EBA has identified some areas where improvements could be made. For instance, for the card fraud breakdown, the category 'Card details theft' has been added. The EBA has also made changes to the fraud types to align them with the general categories in Guideline 1.1. See the response to comment [46].	*Changes to the sub-categories of fraud type in Annex 2, Data breakdowns A to D and F*
[61]	Definition	One respondent queried the relationship between the definition of fraud in the EBA GL and the definition used by the UK Financial Conduct Authority, explaining that the EBA definition was broader and less specific and that it did not specifically include account takeover or fraud related to authorised push payments. The same respondent also noted that the EBA CP refers to 'payment transactions that have been initiated and executed' and does not expressly include 'acquired'. Finally, while the EBA GL indicate that fraud reporting should apply to *all* payment types,	The EBA is of the view that the reference to manipulation of the payer includes the specific category 'authorised push payment' applicable to credit transfers in the UK. The EBA notes that such terminology could not be replicated at European level, as it is not a concept that is easily understood and/or applicable outside of the UK and does not necessarily reflect available technical solutions. The EBA has therefore not followed the suggestion to amend the GL. By contrast, the EBA agrees with the comment about the absence of 'acquired' and has remedied this by amending the definition in Guideline 1.2, as mentioned in the response to comment [49].	*Guideline 1.2:* 'For the purposes of Guideline 1.1 above, 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)**."

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		but only certain payment types are listed, it is the respondent's view that the Guidelines include only some types.	Finally, the GL include all payment types and the EBA clarifies that, for instance, 'instant payments' are a sub-category of credit transfers and should therefore be reported there.	
[62]	Scope	One respondent expressed the view that each PSP should report only the fraud that it is currently experiencing and a statement to this effect in the GL would be welcome.	The EBA agrees with this principle and is of the view that it has followed it in the data breakdowns.	*No change*
[63]	Fraud types	One respondent argued that it would be helpful if the fraud types were aligned with the fraud types identified in other payment industry initiatives.	As mentioned in comments [46] and [60], the EBA has done so to the extent possible in the framework of PSD2 and other relevant EU regulations and directives. In general, however, a number of such initiatives exist across the EU, each of which uses slightly different definitions. So it would be impossible for the EBA to align its terms with all of them at the same time and in every detail.	*Changes to the sub-categories of fraud type in Annex 2, Data breakdowns A to D and F*
[64]	Definition	A number of respondents queried the meaning of the definition of 'executed' payments. More specifically, they queried whether funds that are blocked after leaving the payer's account but before they either leave the PSP or arrive in the payee's account should be considered executed or not.	In the EBA's view, in line with PSD2, a payment cannot be deemed 'executed' if the payment transaction was blocked. The EBA considers there to be no need for further explanation and has therefore not amended the Guidelines.	*No change*
[65]	Definition	A number of respondents suggested changing the terminology 'sender' and 'receiver' to 'issuing' and 'acquiring' sides or something similar, in particular with regard to Guidelines 2.14 and 2.15	The EBA has considered this request and agrees with the respondents that the terms 'sender' and 'receiver' should be replaced with 'issuing' and 'acquiring'.	*Changes throughout the GLs* *For example change of Guideline 2.14 (now 2.11):* "For the purpose of avoiding double-counting ~~as much as possible and maintaining the quality of the data~~, the **payer's** payment service provider should submit data in ~~their~~ **its issuing (or**

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
				initiating) capacity ~~as the sending participant in a transaction~~.”
Feedback on responses to question 3				
[66]	Exclusion of AISPs	Many respondents agreed with the EBA’s proposal not to include AISP providers. Respondents noted that AISPs were also obliged to comply with the EBA GL on major incident reporting and have to report major operational and security incidents they may suffer.	The EBA, in agreement with the respondents, confirms that AISPs have to comply with the EBA GL on major incident reporting, which requires having procedures for both, handling and reporting operational and security incidents in place.	*No change*
[67]	Exclusion of AISPs	Other respondents also agreed with the EBA’s proposal but suggested that the exclusion should also include payment initiation service providers (PISPs) for the following reasons: • PISPs do not hold funds. • PIS and banks do not provide the same services, and so do not possess the same level of information or face the same level of risk. • PISPs do not execute payment services; they only initiate the payment. In other words, they activate a request of the payment service user (PSU) regarding a payment account held at another PSP.	A PISP initiates payment transactions and is part of the payment chain. The EBA is therefore of the view that PISPs must be included in the reporting. This will enable CAs to gain an insight into the amount of fraudulent transactions initiated by a PISP. The EBA is, however, also of the view that the data breakdown required from PISPs should be more limited than a number of other breakdowns on the basis of the information held and proportionality. This is why the CP proposed a more limited Data Breakdown H in Annex 2 for PISPs, which the EBA has decided to retain in the final GL.	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		• PISPs have very limited information on fraud and cannot provide any added value.		
[68]	Exclusion of AISPs	Some of the respondents who agreed with the proposal suggested that specific guidelines be drafted for AISPs or that they should be enabled to do some reporting through other PSPs.	It is the EBA's view that any such reporting should not be included in the EBA GL. However, as mentioned in paragraph 21 of section 3.2 of the Final Report, for overall supervisory purposes, statistical data from registered AISPs may be relevant to CAs, independently from this reporting.	*No change*
[69]	Exclusion of AISPs	Other respondents who agreed with the EBA's proposal to exclude AISPs were, however, of the view that having visibility of incidents against AISPs such as the breach/compromise of customer data was important and that early notification of any such incident should be shared with the rest of the market.	According to the separate EBA GL on major incident reporting, an AISP has to report security incidents to the CA, which in turn will forward the report to the EBA and the ECB. The EBA is of the view that this will provide an opportunity for earlier notification than statistical data would be able to provide under these GL (the GL on reporting fraud data).	*No change*
[70]	Exclusion of AISPs	Other respondents disagreed with the EBA's proposal and argued that it was important for AISPs to report for the following reasons: - to enable authorities and PSPs to learn the potential risks arising from this new type of service; - to evaluate the effectiveness of the provisions made in Article 67 PSD2 (and PSD2 requirements more generally); - to provide information to the market.	The EBA notes that, as mentioned in response to comment [69], AISPs are included in and have to report under the EBA GL on major incident reporting. In addition, the EBA remains of the view that registered AISPs should be excluded, for the purposes of these GL, from the reporting on 'means of payment' in accordance with Article 96(6) PSD2. However, and in line with the response to comment [68], the EBA is of the view that, for overall supervisory purposes, statistical data from registered AISPs may be relevant to CAs, independently from this reporting.	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		Furthermore, they argued that the exclusion of AISPs would cause the following issues: - It would go against the Directive to exclude these providers (Article 33(2) PSD2 in particular). - The reporting could fail to show a key element, such as data and identity theft, that could result in fraudulent transactions. Today, the greatest threats/fraudulent methods start precisely with data/identity theft and social engineering techniques. - Preparatory activity would be omitted from the reporting system. - The effectiveness of the fraud reporting would be fundamentally compromised, as the first point of entry would not be recorded. - Fraudsters are expected to target AISPs. - The reporting would fail to capture the fraudulent use of online credentials in practice. - There may be consistency challenges with GDPR and cyber security regulations. In the view of these respondents, AISPs should report cases where fraudsters have accessed or gathered data for an individual PSU and should also record data with regard		

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		to the cases in which SCA was used versus cases where SCA was not used. Some respondents considered that reporting should be done using similar breakdowns to those required for payments, i.e. whether the user was manipulated or a technical method of attack was used. A number of these respondents suggested that the EBA propose a specific template for fraud reporting by AISPs that would be more suitable to the nature and business activity of these market operators, with an appropriate explanation of how to identify non-authorised fraudulent access or use of a payment account.		
Feedback on responses to question 4				
[71]	Exclusion of attempted fraud	A large number of respondents agreed with the EBA's proposal not to include *attempted* fraud data. Reasons included that: - The resulting reporting requirements incumbent on the PSPs would be even more burdensome. - It would harm the principle of proportionality. - There is little that a PSP can do to influence its rate of attempted fraud. - It could be hard for a PSP to accurately calculate the rate of attempted fraud and	In line with the majority of the responses received, and as stated in the cost-benefit analysis, the EBA considers that including attempted fraud data would entail higher compliance costs and could make the assessment of the information provided more burdensome and disproportionate. Furthermore, the EBA agrees with other reasons expressed by the respondents, such as the challenges in terms of the definition and consistency among PSPs. Nevertheless, as part of the PSD2 requirements, the EBA expects PSPs to monitor the effectiveness of their risk and fraud monitoring systems, including by measuring	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		would therefore be of limited value to CAs, the EBA and the ECB. - It is outside the scope of the Guidelines. A number of respondents also mentioned the lack of a definition, which would prevent the collection of comparable data. Some respondents stated that information on attempted fraud should nevertheless be captured by PSPs for internal purposes and that this is something that could potentially be provided for in future.	the number of fraudulent transaction attempts blocked in an effective manner.	
[72]	Exclusion of attempted fraud	A number of respondents disagreed with the EBA's proposal to exclude attempted fraud, encouraging the inclusion of a high-level breakdown of prevented (as opposed to attempted) fraud figures on the basis that: - It would further enhance and better serve the EBA's objectives by providing a more accurate and comprehensive picture of the scale of fraud and the rate of success in preventing it. - Failure to do so would leave a significant proportion of fraud activity unreported. - It could help in identifying trends and assist other entities that might have different strategies for fraud prevention, or might be more vulnerable to fraud.	See response to comment [71].	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		- It would provide valuable information on the type of attacks that a PSP is suffering during a certain period of time. - Sharing such information would contribute to enhancing the level of preparedness of all PSPs to fight against fraud and better prepare themselves against attacks. - It would add context to the reported gross and net fraud rates. - It would enable CAs to assess the effectiveness of the internal controls of the PSP in blocking transactions before they are executed (one PSP's internal fraud reports show that attempted fraud currently accounts for as much as 98.89% of all gross fraud). - It would enable PSPs to identify underlying weaknesses in the fraud control framework that is used by a large number of PSPs. - Given that, according to the EBA, PSPs must monitor attempted fraud, they should also report it. - It would help to create an understanding of the real fraud risk picture in the EU payment market. - The reporting would not be challenging, as many PSPs already collect these data.		

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
[73]	Exclusion of attempted fraud	A number of respondents suggested changing the reference from 'attempted' to 'prevented' fraud, i.e. the value of the attempted fraud prevented as opposed to the potential value of loss from the victim's account. Others expressed the view that an explicit and unambiguous definition of 'attempted fraud' should be provided, in particular in relation to attempted fraud by customers acting dishonestly.	The EBA has taken note of the different comments and suggestions regarding the concept of attempted fraudulent transactions and agrees to change the terminology to 'prevented fraudulent transactions', so as to make it clearer that it refers to those transactions that were attempted but prevented from occurring. By the same token, the EBA is of the view that this change clarifies the meaning of the reference. The focus of the Guidelines is on executed transactions, and the EBA is of the view that no further definition or detail is needed.	*Guideline 2.5 (now Guideline 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**. ~~Attempted~~ **Prevented** fraudulent transactions that are ~~suspected for fraud and~~ blocked before they are executed **due to suspicion of fraud** should not be included.'
[74]	Exclusion of attempted fraud	To ensure that data on attempted fraud can be made available in the future and to provide value for the whole market, a number of respondents asked the EBA to require CAs to share relevant information on attempted fraud with PSPs in the market and harmonise the rules and procedures for doing so. In order not to delay the implementation of PSD2, the EBA should address this request at a later stage, once these GL are applied in the market.	The EBA considers that this requirement would be outside the scope of the GL. Another EBA legal instrument, however, covers this type of information sharing, but from PSPs to CAs. In particular, PSPs should report to their CA those operational or security incidents, including fraud attempts, that are considered major, providing they meet specific thresholds set out in the EBA GL on incident reporting.	*No change*
[75]	Exclusion of attempted fraud	A number of respondents also expressed the view that if attempted fraud was to be included, it should be excluded for the purposes of the calculation of fraud levels in the context of the TRA exemption.	The EBA notes that prevented fraud is outside the scope of the GL.	*No change*
Feedback on responses to question 5				

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
[76]	Gross and net fraudulent payment transactions	A large number of respondents were of the view that reporting 'gross fraud' rather than 'net fraud' would be more appropriate. They argued as follows: – Collecting data on gross fraud would create an inventory of fraudulent operations that could not be prevented by the PSP, and would have multiple benefits in terms of relevance and feasibility. – It would take into account only real cases of fraud having impacted a payer, excluding fraud attempts thwarted before payment. – It would enable the homogeneous collection of the amount of fraud 'equivalent to the nominal values of payments'. – It would measure the amount of funds misappropriated by fraudsters. – It would facilitate data collection on fraud and the assessment and comparison of performance in the matter of prevention and mitigation of fraud across countries.	The EBA agrees with the view expressed by those respondents arguing that only gross fraud should be reported. The GL no longer refer to net fraud. Indeed, the EBA is of the view that it would be overly burdensome and would not provide any indication of the true net damage or loss incurred by PSPs. Instead, the GL require providers to collect and report data on losses on a cash flow basis. The revised GL introduce separate reporting on losses during the reporting period (irrespective of the link between those losses and the transactions reported for that same given period).	*Articles 1.6(g) and 8.3(g) defining net fraudulent transactions have been entirely deleted.* *The reference to net fraud in GL has been deleted in guideline 7.4 and under the data breakdown under Annex 2.* *A new item on 'losses borne', separate from the actual transactions data has been introduced in the GL reporting framework.* *New guideline 1.6(b) has been introduced:* **'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.'** *New guideline 7.13 has been introduced:* **'The payment service provider providing data in accordance with Data Breakdowns A to F in**

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
				Annex 2 should report all losses due to fraud per liability bearer during the reporting period.' *Separate reporting has been introduced in data breakdowns in Annex 2*
[77]	Gross and net fraudulent payment transactions	A large number of respondents were of the view that the EBA GL should not include net fraud transactions data for the following reasons: - There might be practical difficulties leading to the likelihood of unreliable and misleading data. - Net transactions would be difficult to calculate due to missing data or matching options. - There is a time lag between the fraudulent transaction and recovery (especially for smaller PSPs) and payments may be made in instalments over several years. Recovering funds can take 60 days or more. - Insurance companies or other third parties may not reimburse a PSP on the basis of individual transactions, meaning that recovered funds cannot be reconciled with individual transactions. - The data would not reflect the true net damage or loss incurred by the PSP.	The EBA has reflected on the comments and agrees with the view of the respondents that net fraud reporting should not be included for the reasons highlighted by them. See the response to comment [76].	*See the changes to the Guidelines highlighted in the response to comment [76]*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		- The payer might recover money by a different means (other than through the PSP). - The burden of providing the information outweighs its limited interest. - A study mentioned by one respondent suggests that the difference between gross and net fraud is narrow in terms of value of funds actually misappropriated by criminals. - It would not contribute to the overarching goal of fraud reporting, as the net figure is the measure of effectiveness of another process, i.e. the ability to recover the amounts that are the object of fraud cases, which depends on many factors other than technological aspects, such as interbank cooperation, collaboration with law enforcement, insurance coverage, etc. - Gross fraud seems sufficient to estimate fraud level and meet the requirements of PSD2. - The collection of net fraud data would vary from one PSP to another and would not allow benchmarking of performance on prevention and mitigation of fraud at country level.		

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		- There are too many parameters for fund recovery. - Microprudential supervision: operational risk for banks is already assessed and monitored by the regulator through the operational risk reporting under Basel II. If the EU co-legislators, in further developing microprudential supervisory activity, identify the relevance of analysing net fraudulent data at individual PSP level, the establishment of such a requirement would need to be considered at Level 1; - It would monitor the financial impact of fraud and the need to allocate capital rather than monitoring the effectiveness of prevention and risk reduction measures. A number of respondents explained that several factors of a very different nature cause variations in the 'net fraud' total, namely the extent of funds allocated to amicable or contentious recovery, the extent of reimbursements from insurance, the financial responsibility in the event of fraud as agreed with non-consumers contractually, and the fraudster's or beneficiary's solvency (i.e. if reimbursement can be obtained). Some respondents described net fraud as a 'nice-to-have' rather than an 'essential'.		

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
[78]	Gross and net fraudulent payment transactions	One respondent suggested instead requiring PSPs to provide the monetary value of funds recovered or losses encountered, regardless of when the fraud happened or if it can be assigned to any particular case.	The EBA agrees with this suggestion. The revised GL introduce separate reporting on losses during the reporting period (irrespective of the links between those losses and the transactions reported for that same given period). See the response to comment [76].	*See the changes to the Guidelines highlighted in the response to comment [76]*
[79]	Gross and net fraudulent payment transactions	A number of respondents agreed with the EBA's proposal that both gross and net fraud transactions should be reported, on the basis that it could be a strong enabler in creating transparency and awareness around fraud for the European payment sector as a whole. However, they also highlighted that the recovery of any amount by the PSP may take place in a different reporting period from that in which the fraud case was initially reported and argued that the EBA should provide detail on how such reporting after the event should take place; the maximum extent of the period during which recovery should be reported; and the form these recoveries should take.	Due to the inherent problems with reporting accurate and high quality net fraud and the likely burden, as presented in comments [76] and [77], the EBA abandoned the reference to net fraud, requiring the reporting of data on losses borne on a cash flow basis instead.	*See the changes to the Guidelines highlighted in the response to comment [76]*
[80]	Gross and net fraudulent payment transactions	A number of respondents highlighted that it was necessary to provide more detail and a methodology in relation to recovery, covering previous reports, the exchange rate to be used, the maximum period during which recovery should be reported back and the form to be used.	The EBA came to the decision that the provision of accurate and high-quality data related to the recovery of funds would be very difficult and therefore has abandoned the reference to net fraud and recovery of funds.	*See the changes to the Guidelines highlighted in the response to comment [76]*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
[81]	Gross and net fraudulent payment transactions	Other respondents highlighted that the interpretation of funds recovered was very open and sought clarification from the EBA. They wondered whether it included chargebacks and gross negligence (i.e. customer-borne liability due to negligence).	The EBA came to the decision that the provision of accurate and high-quality data related to the recovery of funds would be very difficult and therefore has abandoned the reference to net fraud and recovery of funds.	*See the changes to the Guidelines highlighted in the response to comment [76]*
[82]	Gross and net fraudulent payment transactions	A number of respondents asked for the definition of 'net fraudulent payment transactions' to be standardised, citing differences between paragraph 31 of section 3.2 of the Final Report and GL 1.6(g) and 8.3(g).	Due to the inherent problems in reporting accurate and high-quality net fraud data, as highlighted in the previous comments, the EBA has abandoned the reference to net fraud. The GL now require the reporting of data on losses borne on a cash flow basis instead.	*See the changes to the Guidelines highlighted in the response to comment [76]*
[83]	Gross and net fraudulent payment transactions	Other respondents were still of the view that the distinction between gross and net loss was not sufficiently clearly explained.	The EBA agreed that the distinction between net and gross loss was not sufficiently precise. The current GL require the reporting of only 'gross' fraud as far as the actual transactions are concerned, as well as separate reporting on losses borne split between the PSP, the PSP's PSU and 'others', reflecting the actual economic damage impacting them. Losses borne may be disassociated time-wise from the actual transactions that incurred them, as there may be a significant time lag between the individual fraudulent transaction and the registering of the resulting economic loss in the PSP's books.	*See the changes to the Guidelines highlighted in the response to comment [76]*
[84]	Gross and net fraudulent payment	Some respondents thought that excluding damages that were refunded by insurance companies was not appropriate either from a	The EBA came to the decision that the provision of accurate and high-quality data related to the recovery of funds would be very difficult and therefore has	*See the changes to the Guidelines highlighted in the response to comment [76]*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
	transactions	national economic viewpoint or for the purpose of statistical comparison. Others thought the recovered amount should only include the amount recovered from the fraudster himself, the rest being irrelevant.	abandoned the reference to net fraud and recovery of funds.	
[85]	Gross and net fraudulent payment transactions	On the basis that the reconciliation and tracking of these could be onerous, with a single transaction potentially subject to two or more adjustments in subsequent reporting periods, some respondents suggested reviewing Guideline 1 and the recording/reference dates. They suggested considering net fraud reporting on a cash flow basis (losses and recoveries recouped during a given period) rather than on an accounting/accruals basis (matching transactions across different periods).	The EBA agrees with the view expressed by the respondents and has abandoned the reference to net fraud, requiring the reporting of data on losses borne on a cash flow basis instead. See the responses to comments [76], [77] and [84].	*See the changes to the Guidelines highlighted in the response to comment [76]*
[86]	Gross and net fraudulent payment transactions	The cost-benefit analysis states that the choice to include net and gross data on fraudulent payments allows CAs to gain information about the effectiveness of the security processes applied by PSPs, which is incorrect. In the respondent's view, it is the fraudulent transactions that are blocked by PSPs that provide an indication of the effectiveness of the security processes applied by PSPs.	The EBA agrees with the respondent to the extent that data on net fraud will not provide information about the effectiveness of the security processes applied. References to net fraud have been deleted from the GL.	*See the changes to the Guidelines highlighted in the response to comment [76]*
[87]	Gross and net fraudulent	Some respondents suggested that if the proposal in the CP was to be maintained, a	The EBA came to the decision that the provision of accurate and high-quality data related to the recovery of	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
	payment transactions	clear distinction between transferred and recovered funds should be made.	funds would be very difficult and therefore has abandoned the reference to net fraud and recovery of funds.	
[88]	Gross and net fraudulent payment transactions	Some respondents highlighted that there was an incorrect cross-reference that should probably be to Guideline 1.6(f) and (g).	Due to the reorganisation of the Guidelines, the numbering has significantly changed. Furthermore, the EBA has removed the reference to net fraud, consequently deleting Guideline 1.6(g).	*Guideline 1.6(g) has been deleted. See the changes to the Guidelines highlighted in the response to comment [76]*
[89]	Gross and net fraudulent payment transactions	One respondent disagreed with the definition of 'gross fraud' and argued that payment transaction that are processed and subsequently reversed within minutes or hours (detected through other systems as fraudulent) should not be included. In these sorts of cases, where the fraudster has not gained and the genuine account holder has not lost, it seems wrong that the transaction should be reported as a gross loss. This approach towards reporting fraud losses affords no credit to asynchronous fraud detection strategies, which are common throughout the industry.	According to the GL' definitions, if a fraudulent transaction has been executed, it will have to be reported as gross fraud, regardless of whether the funds have been recovered afterwards or not. Nevertheless, if the transaction becomes reversed, as suggested by the respondent, the PSP is not to include any loss related to this particular transaction in the overall losses borne figures, which are reported separately. In such cases, the fraudulent transaction has been prevented and therefore is not included in the scope of the Guidelines. See the response to comment [73].	*No change*
Feedback on responses to question 6				

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
[90]	Reporting frequency	A large number of respondents (62%) disagreed with quarterly reporting for a number of reasons, including the following: - Given that the collection is already burdensome, such frequent reporting would dramatically increase reporting/compliance and systems costs for all stakeholders, while the benefits of this frequency might not be substantial. PSPs' resources could better be expended on promoting innovation and user convenience and on fighting actively against fraud instead. - It offers very limited benefits for CAs, since each PSP must already, under Article 96 PSD2, report all major incidents to its CA without undue delay; and under the draft RTS on SCA and CSC (Article 95 PSD2): (i) immediately report to its CA where one of its monitored fraud rates, for any given payment instrument, exceeds the applicable reference fraud rate set by the RTS and (ii) make the results of its fraud monitoring available to the CA upon its request. - Article 96(6) PSD2 refers to at least annual reporting and does not require quarterly reporting, so annual reporting would be fully compliant with the requirements set in this Article.	The EBA has considered these views and has concluded that a balance needs to be struck between supervisory and regulatory needs and the reporting burden on the industry. The EBA, on balance, agrees that quarterly reporting would be too burdensome and agrees with the respondent who suggested a compromise in the form of half-yearly reporting. The EBA considers this to be an appropriate compromise between limiting the burden on PSPs and CAs on the one hand and the need for the EBA and the ECB to have access to relatively timely data on the other. This has led to changes to Guidelines 2.8, 3.1, 7, 9.6 and 10.4, as well as to the deletion of Annex 3. See the response to comment [16].	*Guideline 3.1:* 'The payment service provider should report data **every six months** ~~on an annual basis~~ based on the applicable data breakdown(s) in Annex 2 ~~and data, on a quarterly basis, based on the applicable data breakdown(s) in Annex 3, depending on the service provided and the payment(s) instrument(s) used~~.' *Guideline 3.2:* 'The payment service provider that ~~may~~ benefit**s** from an exemption under Article 32 PSD2 and e-money institutions that ~~may~~ benefit**s** from the exemption under Article 9 **of** Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions (EMD) should ~~only~~ report the ~~full~~ set of data **required in** ~~requested under~~ the applicable form(s) under Annex ~~1~~ **2 only** on an annual basis **with data broken down into two periods of six months**. *Annex 3 has been deleted and the references to quarterly in Guideline 7 and GL 2.8, 3.1, 9.6 and 10.4 have been deleted*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		- The evolution of fraud is relatively slow and annual reporting for all PSPs, be they small or large, is sufficient to analyse trends in fraud. - The reporting will include seasonal effects, including peaks in the amount of transactions (i.e. during the Christmas period), and therefore could result in misleading reports. - Less frequent reporting would limit the need for corrections. - Quarterly data would require a significant amount of resources also from CAs and the ECB and the EBA, and, if they do not have these resources, then PSPs should not be required to report with that frequency. - The data would not be significantly different from draft annual data. - Quarterly reporting would not add any value to the fight against fraud, as fraud detection and mitigation have to be done in a short period of time, much faster than on a quarterly basis, and exceptional cases must already be declared, so the regulator will be informed of any event of systemic importance.		

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		- It would go against the principle of proportionality and would not support the EBA's wider objectives. - Annual reporting would be in line with existing national practices (in a number of Member States) and aligned with Article 96(6) PSD2. - Quarterly reporting would most likely not achieve the outcome expected by the EBA (frequent reporting would not improve quality, instead requiring frequent corrections to previous reports) and would not allow the authorities to draw any meaningful conclusions on the sources or methods of frauds, or any other complex insights into fraud, which cannot be deduced from aggregated data. - The amount and extent of the detail of the data required on a quarterly basis appear to be greater and more costly to implement than would be necessary to calculate the requirements of the RTS on SCA and CSC and, specifically, to apply the TRA. - The linking of the Guidelines to the RTS on SCA and CSC would not make sense in practice and would add another layer of uncertainty to what should be a standard regulatory reporting exercise.		

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		One respondent suggested, as an alternative, that the EBA consider changing the frequency of reporting from a quarterly to a half-yearly basis to ensure more meaningful statistics, and more stable and complete fraud data, while minimising the need for adjustments. A half-yearly frequency would meet the key aim of showing the trends in specific ongoing fraud events, while enabling, for example, a specific focus on types of products or types of attack (data breaches, stolen credentials, specific attack campaigns, etc.). If the half-yearly reporting were the only frequency established by the EBA, this would allow PSPs to set up a single reporting system and have a single timeline to refer to every six months. Some respondents agreed with the quarterly reporting requirement, given the requirements for quarterly data in the RTS on SCA and CSC. - A number of respondents also disagreed with reporting different data in terms of granularity depending on the frequency of reporting.		
[91]	Reporting frequency	A number of respondents disagreed with the exemption from quarterly reporting for small electronic money and payment institutions, on the basis that fraud applies with no exceptions. They argued that fraudsters may focus on smaller institutions if they are	The EBA clarifies that the Guidelines do not exempt small payment institutions and EMIs from reporting fraud data. The Guidelines provide for an exception to the reporting frequency for small institutions. Small payment institutions and EMIs that benefit from an exemption under Article 32 PSD2 or Article 9 of the EMD would be	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		exempted, and that the exemption might constitute a point of vulnerability. These respondents suggested that the CA should have the right to require that such PSPs also report their data every quarter. They also suggested an intermediate solution whereby small PSPs would be required to report on a quarterly basis until the first annual reporting period in 2020.	required to report only annual data. The principle remains in the revised Guidelines.	
[92]	Data breakdown	A number of respondents also disagreed with reporting different sets of data, considering it overly complex and burdensome.	The EBA agreed with these respondents and has revised the Guidelines to require the reporting of the same detailed data, rather than different sets of data with a different frequency, on a semi-annual basis. Guidelines 3.1 and 3.2 have been changed and Annex 3 deleted. See the response to comment [90].	*See the changes highlighted in the response to comment [90]*
[93]	Date of application	A number of respondents disagreed with the suggested starting date on the basis of some of the data not being **available.** In particular, respondents argued that: – Data on PISPs would not be available from April 2018 as the service would 'not yet be available under PSD2 and the respective RTS on SCA and CSC'. – Data on SCA and the relevant exemptions would 'still be in the process of being implemented'; it would not yet be possible to 'tag' transactions as 'SCA' or 'no SCA', or differentiate them on the basis of the exemptions under the RTS.	The EBA considered the arguments against a 2018 starting date to be valid and therefore agreed to postpone the first reporting period. Given the changes expected from market participants, and in particular from those that are not yet collecting similar data under other legislation on payment statistics, the detailed data breakdowns and the implementation work required, the EBA decided to change the date of application to 1 January 2019, with the exception of the data breakdown on exemptions used when SCA was not applied, which will start only from the date of application of the RTS on SCA and CSC on 14 September 2019.	*Paragraph 15 of the GL, under the heading 'Date of application', now reads:* These GL apply from **1 January 2019** ~~13 January 2018~~**, 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.**

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		Overall, a significant number of respondents were of the view that the start of reporting should be delayed, on the following grounds: – the final version of the GL was not yet available; – the 'very limited time' for PSPs to adapt their monitoring systems; – the need to 'tag' transactions on the basis of the final RTS; – the significant IT work required due to different payment channels being located in different systems; – in some countries there have been no comparable reporting requirements whatsoever to date, requiring the development of methodologies, processes and reporting procedures from the scratch; and – potential manual input. Some of these respondents pointed out that the data being sought by the EBA significantly exceeded those currently collected and reported by PSPs, leading to the need for significant investment, especially given the reliance and dependency on matching of data across different systems, the need to liaise with third party software providers and potential changes to scheme data, which will be particularly complex for large PSPs. ⇨ Some of these respondents therefore suggested that the starting		

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		date should be 2019, others 2020 and still others from the time when the RTS apply.		
[94]	Date of application	A number of respondents expressed confusion about the first reporting period, querying the references to H2 2018 and Q2 2018.	The GL now apply from 1 January 2019, with the first period to be reported on being H1 2019. Aggregate data will have to be provided to the EBA and the ECB by CAs at the latest six months after the end of H1 2019, i.e. 31 December 2019.	*See the changes to paragraph 15 of the GL highlighted in the response to comment [93]*
[95]	Date of application	A number of respondents sought clarity on reporting timelines for PSPs to CAs and some disagreed with CAs being allowed the discretion to establish these timelines.	The EBA considers that the GL should not define the timeline for PSPs to provide the data to CAs, given that CAs may have existing payment statistics collection timelines and that this reporting may be integrated with other existing national reporting. Under Guideline 10.4 (now Guideline 3.4), CAs must provide data to the ECB and the EBA within six months after the end of the reporting period.	*No change*
[96]	Reporting open cases	Some respondents argued that the term 'detected' was not appropriate and, in order to avoid confusion and misreporting, they suggested using 'confirmed', 'reported' or 'notified' instead, in line with current industry fraud reporting.	The EBA remains of the view that 'detected' is the appropriate terminology to use given that it encompasses both cases that have been notified or reported to the PSP and cases that the PSP has identified itself.	*No change*
[97]	Reporting open cases	A number of respondents asked the EBA to change the reporting from open cases to closed cases to ensure certainty and clarity and to avoid potential non-fraud cases being included. They also argued that reporting on open cases would require adjustments to past data and that, in conjunction with the quarterly	The EBA is of the opinion that reporting from the time fraud has been detected allows the authorities receiving the data to have a more accurate idea of the security issues closer to the reporting period and allows them to investigate in more detail in a timely manner if necessary. The EBA has retained in the Guidelines the principle of reporting on open cases, allowing the possibility for	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		reporting obligations, it would lead to retroactive reporting regarding recovered amounts, which result in double counting of some transactions.	reporting agents to provide corrections to the figures for those fraud cases that are later found not to be fraud. The EBA is of the view that a risk of overestimating the number of fraud cases is better than the risk of underestimating that would result from reporting on closed cases, which might lead to misjudgement and misinterpretation, as well as a significant time delay.	
[98]	Date of application	A number of respondents were of the view that any retroactive reporting would be of limited value, as the data do not vary a great deal in practice, and would be burdensome for PSPs. Some respondents expressed the view that revised data submissions going back three years were of little use, as they would not allow any analysis of the evolution of fraud methods or the efficiency of measures to combat fraud. Some respondents asked the EBA whether only the updated data for a past period should be sent or whether a new complete report should be sent. They also sought clarity on Guideline 6.3, referring to 'at least up to one year old'.	The EBA notes that it is important to allow revisions of fraud data, as there may be some changes until the case is closed, especially under PSD2, which provides the customer with up to 13 months to report an unauthorised transaction. The EBA agreed that three years was a long period and has concluded that 13 months, in line with PSD2, will be sufficient, as reflected in Guideline 3.2 addressed to CAs. Guideline 6.3 (formerly Guideline 6.4) addressed to PSPs states that they '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'. The exact period is to be defined by CAs.	*Guideline 3.2:* 'The competent authority should report adjustments **to data on any fraudulent payment transaction reported in** ~~for~~ any past reporting period~~s for any fraudulent payment transaction dated up to 13 months old~~ during the next reporting window after the information necessitating the adjustments is discovered **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**~~, by submitting revised data with an explanatory note and within three years~~.'
Feedback on responses to question 7				
[99]	Data breakdown	A number of respondents agreed with the degree of detail required and found it important from a customer communications perspective.	On balance, the EBA has streamlined the reporting to further limit the burden imposed while enabling access to the necessary data (excluding the nice-to-have).	*Changes throughout Annex 2*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
[100]	Data breakdown	A number of respondents highlighted that the geographical breakdown criteria used did not match those used for the statistical data on payments and statistics on card fraud gathered by the ECB.	The EBA agrees that the geographical breakdown was not clearly aligned with the ECB Regulation on payment statistics. For ease of use, the EBA has specified a single geographical area with transactions to be broken down into domestic, cross-border within the EEA and cross-border outside the EEA. See the response to comment [48].	*See the changes highlighted in the response to comment [48]*
[101]	Data breakdown	A number of respondents were of the view that card schemes rather than PSPs should change their current reporting on fraud to comply with these Guidelines and report to CAs, to limit the burden and costs in terms of technology and operations developments for PSPs.	The EBA understands the practical benefits of the proposal from the respondents. However, the EBA notes that PSD2 specifically requires PSPs to collect and report data and that this responsibility cannot be delegated. In addition, a scheme approach would provide piecemeal data, given that many PSPs are likely to use payment instruments other than cards.	*No change*
[102]	Data breakdown	A number of respondents argued that investment would be needed to support data reporting on credit transfers and direct debits, as they are not currently captured by schemes or PSPs.	The EBA appreciates that the change from the current reporting will entail some one-off costs to set up the system.	*No change*
[103]	Data breakdown	Some respondents expressed the view that the plethora of data might be misleading, as the breakdown would not match real-life cases. They further explained that in the absence of automatic collection, the result becomes unreliable and 'in an accumulated form'. They highlighted that many of the data required by the Guidelines are not available today, for instance data broken down by fraud	The EBA acknowledges that the reporting will require one-off systems set-up costs, as well as ongoing compliance monitoring. The EBA is also of the view that more limited requirements regarding data breakdown will contribute to a better balance.	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		type, and argued that, in practice, attacks are usually based on two or more types of these fraud categories. For example, a fraudster may use a technical modification in order to manipulate the payer, or a fraudster may manipulate the payer to gain access to credentials that allow the fraudster to issue a payment order on his behalf. Categories that require further information from a PSU or a (subjective) classification by a PSP employee should be added only after a more thorough consultation process. Where PSP employees are required to assign categories, possibly by questioning PSUs or other parties, procedures and objective criteria need to be developed to specify how PSPs should make such judgments and how unreliable data should be treated.		
[104]	Data breakdown	A number of respondents argued that the payee's PSP would not be able to provide a reason for the application of SCA, given that this decision would have been made by the merchant. They also explained that there was no need to specify the reason for using SCA and pointed out that the reason is not usually associated with any individual transaction.	The EBA agreed with the comments and concluded that the column headed 'Reason for performing SCA' should be deleted.	*The column headed 'Reason for performing SCA' has been deleted from Annex 2, Data Breakdowns A, C, D and F*
[105]	Data breakdown	Some respondents argued that the decision on authentication of non-remote POS payments was a matter decided on by	The EBA agrees that, in the context of cards, decisions on some exemptions will be made by the payee's merchant, with the last word going to the payer's PSP. The use of	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		merchants and information in this regard should therefore be provided by the acquirer rather than the issuer.	exemptions may therefore differ between the payer's and the payee's PSP.	
[106]	Data breakdown	A number of respondents argued that, while the reasons for using non-SCA, distinguishing between remote and non-remote channels, could be interesting, it is likely to be difficult to produce statistics automatically and substantial developments efforts will be needed.	The EBA acknowledges that some of the data are likely to require some changes on the part of the reporting PSPs but is of the view that the information on exemptions and whether a transaction is remote or non-remote is relevant and valuable for supervisors and should therefore be reported.	*No change*
[107]	Data breakdown	One respondent queried the fact that ASPSPs would be reporting fraudulent payments via a PISP in 2018, as they would not always able to determine whether it was a PISP or a PSU making the payment, and argued that ASPSPs should therefore be exempted from reporting that information until the RTS applied.	The EBA agrees that until the RTS apply in 2019 the data reported with regard to PISPs by providers executing credit transfers may be of limited reliability. The EBA, however, remains of the view that such data should be provided to give an insight into the developing market. The EBA also notes that card issuers or acquirers do not have to report data on PISPs.	*No change*
[108]	Data breakdown	A few respondents ask for debit and credit/charge card fraud to be reported separately, given their different profiles and processing set-ups, and because the types of fraud committed may vary.	The EBA agrees that it would be sensible to distinguish between debit and credit cards and Data Breakdowns D3, D4 and E in Annex 2 make this distinction.	*Inclusion of a distinction between debit and credit card data in Data Breakdowns C, D and E in Annex 2.*
[109]	Data breakdown	A significant number of respondents expressed the view that the data breakdown was very burdensome. In particular: – The geographical breakdown was too detailed and too complex, compared with other, similar, categories of data required, as well as entailing a significant additional	With regard to the geographical area, the EBA considered the arguments and agreed to simplify the geographical reporting by consistently using only one geographical area. As a result, Guideline 4.1 has been revised. See the response to comment [48].	*See the changes highlighted in the response to comment [48].*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		workload. They thought that the requirement to break down reported fraud data separately for each EEA country would introduce a significant additional workload for many PSPs that offer their services across the EEA. Some suggested a simple distinction between 'within the EEA' and 'outside the EEA', or between 'domestic/cross-border within the EEA' and 'one leg in or out'. Respondents also highlighted that it was not always possible to correctly identify the country. One respondent argued, furthermore, that there was limited added value in distinguishing between domestic and cross-border data. -The detailed breakdown based on authentication method was too burdensome. In both cases, some respondents suggested that the breakdown in question should not be compulsory.	The breakdown based on the reason for applying SCA has been removed from Annex 2.	
[110]	Data breakdown	A large number of respondents were opposed to reporting a country-by-country breakdown. Some of these respondents queried the reason for requiring a country-by-country breakdown and cautioned against imposing the burden that would be entailed by doing so, arguing that it would be labour intensive and costly; they expressed their preference for the removal of this requirement. Others also highlighted that such a breakdown risked inflating the volume of data	The EBA considered these arguments and revised the GL, which now require only a geographical breakdown of domestic, cross-border within the EEA and cross-border outside the EEA transactions. This has led to the redrafting of Guideline 4.1	*See the changes highlighted in the response to comment [48]*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		and could result in the provision of misleading information.		
[111]	Data breakdown	One respondent asked for the breakdown based on the authentication method (SCA or non-SCA) to be combined with the remote/non remote breakdown for Geo 2 and for the breakdown by payment channel for 'Geo 3' to be removed.	The EBA considered these arguments and revised the GL, which now require only a breakdown of domestic, cross-border within the EEA and cross-border outside the EEA transactions.	*See the changes highlighted in the response to comment [48]*
[112]	Data breakdown	One respondent suggested that some information was missing, namely: – rules to identify and/or avoid the impact of double reporting, especially for card transactions; – rules to identify and/or avoid the impact of later corrected volumes/values (due to early reporting); – rules for multiple possibilities to avoid multiple reports (e.g. a payment can be exempted for more than one reason); – separate channels or types (e.g. a distinction between credit institutions and payment institutions); – cash-in or -out channels only were not sufficient, as remittance covers cash-in *and* -out channels; The respondent suggested combining all the separate tables into one flat structure.	The EBA is of the view that the suggestions for further clarification and detail on implementation cannot be added to the GL but could be addressed through the Q&A tool once the process has been formally implemented. The EBA clarifies that cash withdrawals are not within the scope of the GL and has decided to add a category of breakdown (Data Breakdown E) for cash withdrawal.	*New Guideline 7.14:* **Payment service providers reporting card payment transactions in accordance with Data Breakdowns C and D in Annex 2 should exclude cash withdrawals and cash deposits.** *New Data Breakdown E in Annex 2*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
[113]	Data breakdown	Some respondents suggested removing the fraud types and enriching the breakdown tables in accordance with the SCA or non-SCA authentication method. Respondents suggested that breakdowns based on the authentication method (SCA or non-SCA) should be combined with the remote/non remote breakdowns for Geo 2. In their view, this would enable better identification of the operating modes. They argued that the fraud types should be removed because the difference between different types is more legal than operational and often misunderstood by managers, and they would impose a significant administrative burden. With regard to manipulation of the payer to issue a payment order, they were of the view that the payer was unlikely to admit he had been manipulated out of fear of that a refund would be denied. Instead, they suggested 'automated measurement of the fraud supplemented by a qualitative analysis of the procedures'.	The EBA disagrees with the views of those respondents suggesting not reporting any data by fraud type. The EBA is of the view that fraud types are essential in order to understand, for instance, new trends in fraud, the most common fraud types, etc. The fraud types therefore remain in the Guidelines.	*No change*
[114]	Data breakdown	One respondent was of the view that for PISPs Tables 3 and 4 on page 37 should be grouped together.	The EBA has made a number of changes to Data Breakdown C for PISPs.	*Changes to Data Breakdown H in Annex 2; the data breakdown by instrument has been simplified*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
[115]	Data breakdown	A number of respondents were of the view that not all broken down data could be provided. For example, the location of the acquirer or the location of the payee's payment account is currently not collected, as all credit card transactions are settled through card schemes and not directly with the acquirer.	The EBA is of the view that the GL are likely to require a number of changes, including that providers will have to start collecting data that they do not currently collect.	*No change*
[116]	Data breakdown	A significant number of respondents were of the view that general guidance on the methodology for fraud reporting should be provided centrally by the EBA, as opposed to by CAs, to ensure a harmonised approach and consistent timelines across the EU.	The EBA is of the view that detailed implementation questions are outside the scope of the GL, but agrees that this is something that the EBA may wish to address.	*No change*
[117]	Data breakdown	One respondent was of the view that one of the exemptions to SCA, on credit transfers between accounts held by the same natural or legal person, was missing and should be added.	The EBA notes that this is covered by 'payment to self'.	*No change*
[118]	Data breakdown	One respondent expressed concerns about some of the reporting, especially with regard to PIS. The respondent was of the view that the payee's PSP may not be able to detect that the entity that initiates a transaction is a PISP acting on behalf of the payer rather than the payer's ASPSP. The respondent also suggested that, where the payee's PSP itself acts as a PIS, it may be particularly confusing.	The EBA agrees that until the RTS apply in 2019 the data reported with regard to PISPs by providers executing credit transfers may be of limited reliability. The EBA, however, remains of the view that such data should be provided to give an insight into the developing market. The EBA also notes that card issuers or acquirers do not have to report data on PISPs.	*Changes to Annex 2, Data Breakdowns D3 and D4 (now Data Breakdowns C and D); references to transactions via PISPs (Tables A7 and A6) have been deleted*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		The respondent therefore suggested that the payee's PSPs not be required to report PIS-initiated transactions.		
[119]	Data breakdown	One respondent sought greater clarity on the reporting for money remitters, asking in particular for confirmation of whether 'account-based money transfers', where the agent on the sending side authenticates consumers by requiring them to log in to access their account, should be reported as credit transfers or as money remittances.	Guideline 1.3 states that, in the case of money remittance services where funds were transferred from a payer's PSP to a payer's money remitter PSP (as part of a money remittance payment transaction), it is the payer's PSP, rather than the money remitter PSP, who should report the payment transactions from the payer's PSP to the money remitter.	No change
[120]	Data breakdown	A number of respondents explained that acquirers only detect fraud where losses are charged back.	The EBA acknowledges the potential limitation in terms of reporting but is of the view that the requirement for acquirers to report should remain in the GL.	*No change*
[121]	Data breakdown	As recurring card-based payments are repeatedly drawn by the payee from the card account of the payer and are based on an authorisation of the payer by the payee, one respondent considered a recurring transaction to be fraudulent when the authorisation was fraudulent. If one of the subsequent particular payments is disputed for reasons relating to the underlying business transaction, this would not be considered fraudulent.	The EBA is of the view that a recurring transaction could be fraudulent at a stage other than the authorisation stage. Guideline 6.1 states that, in the case of a series of transactions, the date recorded should be the date when each individual payment transaction was executed.	*No change*
[122]	Data breakdown	Several respondents pointed out that it was not possible to identify the location of the payee's PSP/the card acquirer through the data and automated IT mechanisms that are	The EBA appreciates that there may currently be technical limitations that will need to be addressed. The EBA also notes that a country-by-country data breakdown is no longer required.	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		available for issuers in the credit card schemes MasterCard and Visa.		
[123]	Data breakdown	Others were of the view that, for the purposes of fraud reporting in the card payment market, the location of the payee's PSP was irrelevant. The respondents suggested including reporting on the payee's location instead. The location of the relevant payee or POS is much easier to trace than the location of the payee's PSP/the card acquirer, and it would provide a better understanding of the locations where fraud actually occurs.	The EBA agrees that the primary indicator should be the location of the payee for non-remote card payments. This is particularly relevant for country-by-country data, which are no longer required under the GL.	*No change*
[124]	Data breakdown	A number of respondents asked for further clarification on the exact meaning of the 'location of the fraud'.	The EBA is of the view that the sufficient level of detail is included in Guideline 1.6(a) to (f).	*No change*
[125]	Data breakdown	One respondent suggested that the data breakdown for credit transfers for transactions where TRA was used should differentiate only between transactions above and below the threshold of EUR 500.	The EBA agrees that monetary thresholds would probably have been too burdensome, with limited added value for supervisors, and all monetary thresholds under the Article 18 TRA exemption have as a result been deleted.	*Change to Annex 2, Deletion of tables 4.2.1.a under Data Breakdown A, D1 and D4 [now data breakdown C, D and F] and table 5.2.1.a under Data Breakdown D3 [now data breakdown C].*
[126]	Data breakdown	One respondent was of the view that many payment processing systems are not capable of differentiating between online, paper-based and mail order/telephone order (MOTO) transactions.	The sub-categories 'paper' and 'MOTO' have been removed from the GL The reporting now distinguishes only between electronic and non-electronic transactions.	*Change to Annex 2, Deletion of Table B in Data breakdown D1, D3 and D4 [Now Data Breakdown A, C and D]*
[127]	Data breakdown	One respondent asked for every field in the annexes to have an explanation on how it should be filled in. With regard to card reporting, the respondent specifically queried if payment transactions	While the EBA acknowledges the merit of practical explanation, explanations for each field cannot be provided in the GL. In addition, it is not possible to further	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		should include all types of card transactions (ATM, POS, e-commerce, etc.), the difference between remote and non-remote, the definition of 'SCA', etc.	define 'remote' or 'SCA', given that both terms are defined at Level 1 in PSD2.	
[129]	Data breakdown	One respondent queried whether Article 7.9 should be reworded to allow for product-level segmentation, and if Annex 3 should allow for SCA TRA exemption thresholds to be applied at product level.	The EBA considered these queries and arrived at the view that the recording of fraud data should: (i) contribute to assessing the effectiveness of applicable regulations, identifying fraud trends and potential risks, assessing and comparing fraud data between different payment instruments; (ii) enable PSPs to better assess security incidents or emerging fraud trends and threats and contribute to monitoring fraud, including by type of service and payment instrument. Therefore, the data should be collected by payment instruments and not by payment products.	*No change*
[130]	Data breakdown	Another respondent expressed the view that Data Breakdown D3, Table A5.1, and Data Breakdown D4, Table A4.1, seemed problematic, as the categorisation of the rows did not seem clear.	The breakdown has been deleted	*No change*
[131]	Data breakdown	One respondent was not clear about whether cash withdrawals were included in the reporting or not.	The EBA clarifies that cash withdrawals are within the scope of the Guideline, but only cash withdrawals through cards. The EBA agrees that this may not have been clearly stated in the draft Guidelines. For transparency, the EBA has included a new Data Breakdown E for cash withdrawals by card.	*New guideline 7.15:* **The payer's 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 ('cashback') using a card.**

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
[132]	Data breakdown	Some respondents were unsure how they would be able to distinguish between SCA and non-SCA transactions.	The EBA is of the view that a number of changes will need to be applied to PSPs' existing systems in order to report and collect the required data.	*No change*
[133]	Data breakdown	One respondent queried the accuracy of fraud data generally, given that there is no certainty that fraud has occurred in the absence of objective evidence, such as the results of a police investigation. The respondent was also of the view that the data would result in underestimation of the occurrence of fraud.	Fraudulent payment transactions should be reported as soon as fraud is detected in order to allow CAs and PSPs access to timely and fairly accurate data. PSPs should report 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.	*No change*
[134]	Data breakdown	One respondent suggested adding the category 'card number usurpation', as this is the most frequent type of fraud encountered in online payments and should not be included in the 'other' category.	The EBA agrees and has added this category, although it is referred to as 'card details theft'.	*Change to Annex 2*
[135]	Data breakdown	A number of respondents asked for clarification regarding the various geographical breakdowns, especially regarding 1 and 2.	The revised EBA GL require only a geographical breakdown of domestic, cross-border within the EEA and cross-border outside the EEA transactions.	*See the changes highlighted in the response to comment [48]*
[136]	Data breakdown	One respondent was confused about the requirement for transactions and fraudulent transactions data and asked whether in Data Breakdown D1 Tables A2 onwards must be replicated.	The reporting format in Annex 2 has been changed to make it clearer.	*Change to Annex 2*
[137]	Data breakdown	Another respondent highlighted that it is not always appropriate or practical to consider each and every transaction as a separate case of fraud. If the data from a card is intercepted or the card is forged and then used to make a	The EBA considered these arguments and arrived at the view that to report transactions by grouping them under the same fraud event would not offer a clear picture of how efficient a PSP's monitoring mechanisms are.	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		number of transactions before it is blocked, it is more appropriate to add the amounts and group them under the same fraud event, as they relate to the same card and the same breach. Similarly, it is unclear, where fraud is committed against multiple customers through a single case of tampering with a POS/ATM or a single instance of unauthorised access to a system (of the PSP or a third party), whether or not this should be counted as a single event for the purposes of the fraud reporting data collection.	Therefore, the principle remains that PSPs should report on a transaction-by-transaction basis.	
[138]	Data breakdown	One respondent asked for alignment of the terms 'EEA Cross-border transactions' (page 22 of the CP) and 'Cross-border within the EEA' (page 33 of the CP).	The EBA has made the terminology used consistent throughout the Guidelines.	*Changes throughout the Guidelines*
[139]	Data breakdown	One respondent argued that PISPs cannot initiate direct debits or card transactions and therefore suggested that these should be deleted.	The breakdown has been changed. Under the revised Guidelines, data reported by PISPs in accordance with Annex 2, Data Breakdown C (now H), should be broken down only into credit transfers and others.	*Change to Annex 2, Data Breakdown H*
[140]	Data breakdown	One respondent suggested that, should the EBA decide to require the collection of data on the cases specified in Guideline 1.1(b) and (c), these fraud types could be managed separately to gain a clearer and more consistent picture of the effectiveness of the security measures put in place by PSPs.	The fraud type included in Guideline 1.1(b), payer acting fraudulently, has been excluded from the fraud taxonomy set out in the Guidelines. With regard to the other categories, the reporting distinguishes between the two remaining categories, but not for every data point.	*Change to Annex 2, Data Breakdown H*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
[141]	Data breakdown	One respondent suggested that it would be useful to provide practical examples and an operating compilation guide, together with a dedicated taxonomy.	The EBA may wish to consider providing such documents at the implementation stage of the Guidelines once they have been adopted.	*No change*
[142]	Data breakdown	Another respondent suggested removing the contactless and unattended terminal exemption from the credit transfer data breakdown, as the view was that such transactions did not exist.	These types of transactions are specified in the provisions of Articles 11 and 12 of the RTS on SCA and CSC. These exemptions are channel-agnostic, meaning that, while there may not be business models catering for additional options, they should not be excluded.	*No change*
[143]	Data breakdown	A few respondents highlighted that the ASPSP would not be able to provide data on PISP-initiated transactions, given that there is no requirement for identification until the RTS apply.	The EBA considered this argument and arrived at the view that ASPSPs should report fraudulent payments via a PISP on a best-effort basis until the RTS become applicable, as they will not always be able to determine whether it is a PISP or a PSU making the payment.	
[144]	Data breakdown	References to the articles of the RTS on SCA and CSC should be updated.	The EBA has updated the references.	*Changes in references to the relevant articles of the RST on SCA and CSC*
[145]	Data breakdown	A large number of respondents were concerned about the different geographical breakdowns. Some suggested keep Geo 3 for everything; others using Geo 2 only; others still suggested distinguishing between EE and non-EEA transactions without making a distinction between cross-border and domestic transactions; and one respondent suggested expanding the country-by-country breakdown to all countries, rather than just EEA countries, on the basis that the additional work would be minimal.	The EBA considered these arguments and revised the GL, which now require only a geographical breakdown of domestic, cross-border within the EEA and cross-border outside the EEA transactions. See the response to comment [48].	*See the changes highlighted in the response to comment [48]*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		Some of these respondents also expressed concerns about the articulation between the different levels and detailed 'Geo 3' while sums may be at 'Geo 1' or 'Geo 2'.		
[146]	Data breakdown	One respondent asked for more clarity on the distinctions between the data required in quarterly reporting and those required in annual reporting.	The revised GL no longer require quarterly data reporting.	*Annex 3 has been deleted*
[147]	Data breakdown	One respondent queried whether transactions in a currency other than that used by the Member State in question should be considered domestic payment transactions if the payer's and the payee's PSPs are located in the same Member State.	The geographical breakdown does not take into account currency when considering whether a payment transaction is domestic or not. The definition of 'domestic' is included in Guideline 1.6(b) and (c).	*No change*
[148]	Data breakdown	One respondent explained that the determination of whether a transaction are SCA or non-SCA and of the reasons for the decision is made in real time and not stored as part of the transaction information. The respondent also highlighted the fact that one-leg-in/-out transactions are not within the scope of SCA but are still to be reported on the data breakdown. The respondent also queried whether all cross-border transactions need to be reported with a breakdown by country for EEA countries. The respondent also queried whether a transaction was domestic if the payer's and	The EBA agrees that the reporting may require some changes to existing systems. The EBA is of the view that including one-leg-out transactions will provide valuable information. The revised Guidelines require only a geographical breakdown of domestic, cross-border within the EEA and cross-border outside the EEA transactions. See the response to comment [48]. The definition of 'domestic transactions' is provided in Guideline 1.6(a) and (b).	

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		the payee's PSPs were located in the same Member State. The respondent mentioned that paragraph 24 of section 3.2 of the Final Report refers to placing funds falling under PSD2 and queried where these should be reported. The respondent also highlighted that a country-by-country breakdown is not specifically required under Guideline 4. The respondent asked for the requirement for distinction between remote and non-remote for transactions falling under different types of exemptions to be deleted, arguing that it was unnecessary. The respondent finally asked for clarification of the meaning of 'SCA and non-SCA authentication methods' in the context of fraud reporting.	The EBA is of the view that placing funds should not be included. The country-per-country breakdown has been deleted. The requirement for a distinction between remote and non-remote for transactions falling under different types of exemptions has been deleted. 'SCA' and 'non-SCA' refer to the definition of 'SCA' under PSD2 and the obligations under the RTS that will apply from September 2019.	*Changes to the geographical breakdown as highlighted in Annex 1* *Changes throughout Annex 2*
[149]	Data breakdown	A number of respondents ask for clarification regarding the use of the term 'MOTO'.	The EBA notes that this term has been deleted from the Guidelines.	*See the response to comment [58]*
[150]	Data breakdown	A number of respondents were of the view that the types of fraud for card reporting did not correspond to existing codes for fraud defined by card schemes.	See the response to comment [60].	*No change*
[151]	Data breakdown	A number of respondents expressed concerns about the differences in the concept of 'domestic' depending on the payment	The EBA disagrees with the comments and is of the view that explanations are provided in the Guidelines.	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		instrument and channel, as specified in Guideline 1.6: – for non-card-based payments and remote card-based payment transactions, 'domestic' refers to situations where the payer's PSP and the payee's PSP are both in the same Member State; – for non-remote card-based payments, 'domestic' means 'where the issuer, the acquirer and the location of the point of sale (POS) or automated teller machine (ATM) used are located in the same Member State'. The respondents were of the view that this geographical breakdown was not consistent with other explanations, as it ignores cases in which the terminal (ATM or POS) is in a different Member State from the issuer and acquirer. It also presents issues when the payer's PSP and the terminal are both Member States but the payee's PSP is outside the EEA, for example in Switzerland, or where the payee's PSP and the terminal are both in Member States but the payer's PSP is not. Some of these respondents asked the EBA to clarify the geographical breakdowns for non-remote card-based transactions. Others asked the EBA to define 'domestic' solely based on the location of the issuer and location of the POS or ATM on the acquiring side.		

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
[152]	Data breakdown	One respondent expressed concerns about the mismatch between the EBA Guidelines, referring to EEA countries, and the ECB Regulation on payment statistics, which focuses on the EU only.	See the response to comment [10].	*No change*
[153]	Data breakdown	One respondent expressed the view that the low-value exemption should apply to the payee's PSP as well as the payer's PSP.	The EBA agrees and these exemptions have been included in the final Guidelines in Annex 2, Data Breakdown D.	*Additional row in Data Breakdown C under exemptions (formerly Data Breakdown D4)*
[154]	Data breakdown	Another respondent asked for clarification regarding the TRA exemption and whether the payee's PSP should report instances where the issuer uses this exemption and the link with liability under Article 74(2) PSD2.	The EBA clarifies that the payee's PSP should report under the TRA exemption only those cases where the payee's PSP has used this exemption (the decision made by the payer's PSP is not relevant).	*No change*
[155]	Data breakdown	One respondent argued that recurring transactions are not relevant and should not be counted given that they are initiated by the payee and not the payer and therefore not within the scope of SCA.	The EBA is of the view that card transactions are initiated by the payer through the payee and are therefore within the scope of SCA, as explained in the Final Report on the draft RTS on SCA and CSC.	*No change*
[156]	Data breakdown	Another respondent argued that direct debits should be excluded, as they are payee-initiated and therefore within the scope of SCA.	While direct debits are indeed outside the scope of SCA, they are important payment instruments and fraud may take place. The EBA has therefore deleted the SCA breakdown but kept the general table for direct debits.	*No change*
[157]	Data breakdown	One respondent queried what non-remote credit transfers initiated electronically were and suggested this might need to be deleted.	It is the EBA's understanding that, for instance, in some countries credit transfers can be initiated at the POS.	*No change*
[158]	Data breakdown	One respondent queried whether the payee's PSP would have the information on the form	The question of consent is outside the scope of these Guidelines.	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		of consent and suggested it might need to retrieve this from the payer's PSP.		
[159]	Data breakdown	One respondent was unclear about the type of fraud the following case should be reported as: the fraudulent payer has given stolen payment data to the payee in order not to be debited.	As mentioned in comment 41, the revised GL fraud resulting from the payer being a fraudster should no longer be reported. On that basis, the case mentioned by the respondent should not be reported.	*See the response to comment [41] in reference to the deletion of former Guideline 1.1.b*
[160]	Data breakdown	One respondent was unclear about the specific fraud cases that correspond to 'modification of a payment order by the fraudster' or 'manipulation of the payer to issue a payment order' for card payments and how they can be identified. In the respondent's view, card issuers only register the fraud type corresponding to 'card not present' transactions, without any other details. The respondent also suggested that the payee's PSP would not know whether SCA had been applied or not. In the respondent's view, it would not be possible to fill in any of Table A4 (page 44).	The EBA is of the view that the Guidelines may require providers to adapt their systems.	*No change*
[161]	Data breakdown	One respondent suggested that PSPs would not be able to report the information contained in Table A7 of Data Breakdown D3 or Table A6 of Data Breakdown D4 in Annex 2, i.e. initiation of card-based transactions via PISPs.	The breakdown has been deleted.	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
[162]	Data breakdown	Table 4.2. in Annex 2, Data Breakdown D4, requires payees' PSPs to report the reasons for authentication via non-SCA. The respondent suggested deleting the category 'recurring transaction' as recurring transactions are not initiated by the payer. The respondent also suggested deleting references to the TRA exemption on the basis that it could not be used by payees' PSPs.	Recurring card transactions, like card payments more generally, are initiated by the payer through the payee. Therefore, the EBA is of the view that this category should not be deleted. The EBA also clarifies that the TRA exemption may be used by the payee's PSP.	*No change*
[163]	Data breakdown	One respondent highlighted the erroneous blank line or typo in Table A5.2.1.a, Annex 2, 'Transaction intervals', page 42.	The EBA has addressed this formatting issue.	*Change to Annex 2*
[164]	Data breakdown	Given that direct debit recalls can happen over a long period (eight weeks unconditional, 13 months with evidence), this is likely to lead to updates to previous reporting periods.	As specified in paragraph 20 of section 3.2 of the Final Report, refunds under eight weeks should not be automatically reported, as they do not always indicate fraud cases; such transactions should be reported only if they were subject to fraud and the reporting PSP was aware that this was the case, without implying any legal obligation to ask the payment service user whether this was the case.	*Clarification provided in paragraph 20 of section 3.2*
Feedback on responses to question 8				
[165]	Double counting and double reporting	A number of respondents agreed with the EBA that the Guidelines achieved an acceptable compromise between the competing needs to receive comprehensive data and minimise double counting and double reporting.	The EBA concurs with the view expressed by these respondents.	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
[166]	Double counting and double reporting	One respondent queried whether on-us transactions (i.e. transactions where the payer and the payee use the same PSP) were included.	It is the EBA's view that PSPs should report all total and fraudulent payment transactions, including on-us transactions, that have been initiated and executed and/or acquired.	*No change*
[167]	Double counting and double reporting	Some respondents argued that, given the lack of information, rare data sharing and risk of double reporting and double analysis, PISPs should be exempt from reporting fraud information in order to ensure the efficiency of the framework.	Please see the response to comment [67].	*No change*
[168]	Double counting and double reporting	One respondent did not agree with the requirement for PSPs to retrospectively restate net losses, as money is recovered with regard to any past reporting period at least up to one year old.	The EBA came to the decision that the provision of accurate and high-quality data relating to the recovery of funds would be very difficult due to the lack of harmonised practices for recording such data, and has therefore abandoned the references to net fraud and recovery of funds.	*All references to net fraud and recovery of funds have been removed*
[169]	Double counting and double reporting	One respondent suggested referring to 'initiation' and 'acquiring' rather than 'sender' and 'receiver'.	Please see the response to comment [65].	*See the response to comment [65]*
[170]	Double counting and double reporting	To avoid double counting in the area of cards, one respondent suggested that the issuer report fraud for transactions outside the EEA while the acquirer report for all its merchants within the EEA. Other respondents suggested that only the initiating side (card issuer) should report.	The EBA is of the view that, in order for CAs to be in a position to obtain a comprehensive view of fraudulent transactions in card payments, the PSP of both the issuer and the acquirer should report data. This will prevent CAs having only a partial view of any fraudulent payment flow and enable them to more comprehensively capture and identify the origin, source and destination of fraudulent payment transactions.	*Guideline 3.1 in the GL addressed to NCAs* 'The competent authority should report the **volumes and** values of payment transactions and fraudulent payment transactions in line with GL 2.1 and 2.2. To avoid double counting, data should not be aggregated across **the** different **data breakdowns in Annex 2** ~~payment service categories~~**.'**

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		They explained that varying data quality and interpretation ambiguities as well as differing time delays between the payer's and the payee's PSPs might lead to different numbers and thus unclear double counting calculations. Others simply asked for greater clarity and examples to show why both sides should report.	Guideline 3.1 of the Guidelines addressed to CAs clarify that the data obtained from the issuer's and the acquiring side should not be added to ensure that there is no double counting. Guideline 3.1 has been slightly rephrased for clarity.	
[171]	Double counting and double reporting	Focusing on payments from money mule accounts (i.e. accounts created for the sole purpose of transferring money that is the product of crime), one respondent argued that such payments could be subject to double counting. A payment leaving an account could be reported as third party fraud and the same funds could subsequently be reported as first party fraud at another end point.	See the response to comment [44]. The EBA notes that first party fraud is no longer part of the reporting and that, as mentioned in the response to comment [170], CAs are not to add the data received across the different data breakdowns. It is therefore the EBA's view that the risk of double counting would be minimal.	*No change*
[172]	Double counting and double reporting	One respondent argued that transfers between two internally held accounts by the same customer should be excluded to avoid double counting.	It is the EBA's view that PSPs should report all payment transactions and fraudulent payment transactions that have been initiated and executed (including acquired). This includes transfers between two internally held accounts by the same customer. The EBA also notes that there is a specific exemption from applying SCA for such transactions and that data on the use of such exemptions is to be reported under Data Breakdowns A, C, D and F.	*No change*
[173]	Double counting and	One respondent expressed the view that the payee's PSP, in the case of money remittance or e-money transactions under GL 1.3 to 1.5,	As explained in the GL, the data to be reported by the money remitter includes only transactions where funds have been transferred by a money remitter PSP from its	*Guideline 1.3:* In the case of money remittance services where funds were transferred from a payer's payment

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
	double reporting	should not report, on the basis that no further evidence could be gained through double reporting.	accounts to a beneficiary account and e-money transactions. It is therefore the EBA's view that no double reporting will take place. Guidelines 1.3 to 1.5 have been amended to provide more clarity.	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 ~~as the former executed the payment transaction~~. ~~These~~ **Such** transactions should not be reported by the payment service provider of the beneficiary **of the money remittance payment transaction**. *Guideline 1.4:* T~~he t~~ransactions 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 ~~via the form~~ **in accordance with Data Breakdown G in Annex 2**~~/F~~. ~~These transactions should not be reported by the payment service provider of the beneficiary.~~ *Guideline 1.5:* T~~he t~~ransactions and fraudulent transactions where e-money ha~~ves~~ been transferred by an e-money provider to a beneficiary account, including ~~the case~~ where the payer's **payment service provider** ~~PSP~~ is identical to the payee's payment service provider, should be reported by the e-money provider **in accordance with** ~~using~~

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
				Data Breakdown **F ~~A~~ in Annex 2~~/E~~**. Where the **payment service providers** ~~PSPs~~ are **different** ~~distinct~~, payment is ~~only~~ reported **only** by the payer's PSP to avoid double counting.
[174]	Double counting and double reporting	One respondent expressed the view that there was a risk of double counting when reporting the fraud types 'modification of a payment order by the fraudster' and 'issuance of a payment order by the fraudster'. In the respondent's view, in both cases, the payment order has not been issued by the payer. The respondent invited the EBA to clarify that 'modification of a payment order by the fraudster' is only a sub-type of 'issuance of a payment order by the fraudster'.	The EBA disagrees with the respondent that 'modification of a payment order by the fraudster' is only a sub-type of 'issuance of a payment order by the fraudster'. In the EBA's view, the categories are mutually exclusive and refer to two different processes, one relating to issuance and the other to modification (i.e. the issuance was not fraudulent). The EBA therefore disagrees that any double counting will take place.	*No change*
[175]	Double counting and double reporting	One respondent asked for further clarification on how to avoid double counting when aggregating data.	The EBA is unclear on what the respondent means by 'aggregating' data. Data aggregation in the GL refers to CAs aggregating data from all PSPs to provide anonymised data to the ECB and the EBA.	*No change*
[176]	Double counting and double reporting	One respondent asked for clarification on whether the acquirer is required to report all fraud where it has observed an alleged financial loss or only in cases where it receives a notification from the user.	Guideline 6.2 states that PSPs 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.	*No change*
[177]	Double counting and	One respondent expressed confusion about how to identify where to deduct double reporting from the payee's PSP side.	The EBA is of the view that the payee's PSP should not need to deduct any transactions, given that any double reporting would take place through different providers	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
	double reporting		reporting, rather than through reporting from the same provider.	
[178]	Double counting and double reporting	A number of respondents suggested clarifying that only the ASPSP (i.e. the payer's PSP) should report whenever a fraudulent transaction is executed; PISPs and the payee's PSP should not report.	The EBA acknowledges that PISPs' data may increase the risk of double counting and that therefore PISPs data should be reported individually under a separate heading from the data of the ASPSP. The number or value of transactions that are recorded under different headings should not be summed, eliminating the risk of double counting.	*No change*
[179]	Double counting and double reporting	One respondent expressed the view that PISPs should report data but that the payer's PSP should not to avoid double reporting.	In the EBA's view, the PSP reporting credit transfers should report the amount of those that were initiated by PISPs. These data would not be summed with data from PISPs by CAs under Guideline 3.1 of the Guidelines to CAs (see the response to comment [170]), and it is therefore the EBA's view that there no double counting will take place.	*No change*
[180]	Double counting and double reporting	Another respondent explained that fraudulent transactions where an SCA was required (e.g. 3D Secure) cannot be charged back and will always be reported as fraud only by a payer's PSP, suggesting that perhaps the focus should therefore be on the payer's PSP reporting rather than the payee's PSP.	The EBA notes that for most payment services (credit transfers, e-money operations and others) only the payer's PSP is required to report data in its issuing (or initiating) capacity (with the exception of card payments data and PISPs' data), and there is no requirement for the payee's PSP to report. Further clarification has been provided in Guideline 2.11.	*Guideline 2.11:* For the purpose of avoiding double-counting ~~as much as possible and maintaining the quality of the data~~, the **payer's** payment service **provider** should submit data in~~ their~~ **its issuing (or initiating) capacity** ~~as the sending participant in a transaction~~. As an exception, **data** for card payments~~, data~~ should be **reported both by the** ~~submitted by payment service providers in their capacity as both~~ payer's payment service provider ~~(i.e. counted on the issuing side in the country where the transaction originates)~~ and **by the** payee's payment service provider **acquiring the payment transaction** ~~(i.e. counted on the~~

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
				~~acquiring side in the country in which the transaction is received)~~. The two perspectives should be reported separately, with different **breakdowns** ~~forms~~ as detailed in Annex~~es~~ 2 ~~and 3 respectively~~. **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.** ~~competent authorities may wish to require both acquirers and sub-acquirers to report and to do so separately~~. **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.**
[181]	Double counting and double reporting	Another respondent still highlighted the risk of overreporting of fraud transactions through multiple PSPs (payer ASPSPs, PISPs acting on behalf of the payer or the payee, PSPs acting as transactions acquirers on behalf of the payee), with a specific emphasis on PISPs being affected by 'overreporting'.	See the responses to comments [180], [170] and [179].	*No change*
[182]	Double counting and double reporting	One respondent highlighted that the requirement to report both gross and net fraudulent transactions would lead to further overreporting of fraudulent transactions.	As mentioned in the responses to comments [76] and [77] the EBA has concluded following the responses received to the consultation that net fraud should not be reported.	*Deletion of references to net fraud in Guidelines 1.6(g), 2.4, 7, 8.3(g) and 9.4, as well as Annex 2 in all the data breakdowns*
[183]	Double counting and double reporting	One respondent queried which data breakdown a PSP that is both acquirer and issuer should use.	A PSP that is both acquirer and issuer should report different data under Data Breakdowns C and D, depending on the service provided.	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
[184]	Double counting and double reporting	Another respondent queried whether the acquirer should report a fraudulent payment transactions when an economic loss is detected or only when it receives a PSU's notification.	PSPs should report fraudulent payment transactions that have been executed, regardless of whether any financial loss has been incurred.	*No change*
[185]	Double counting and double reporting	Another respondent still cautioned against theoretical clear-cut delineations between the different categories, arguing that they may not always be clear in real-world scenarios. For example, in a scenario where a bank acting as a money agent in the transaction chain, is subject to hacking or a cyber-breach that results in funds being sent out of a bank account through a money remitter, who would have to report? The bank or the money remitter?	Please see the response to comment [173].	*No change*
[186]	Double counting and double reporting	One respondent argued that reporting on payment transactions was already required under the ECB Regulation on payment statistics (Regulation EU 1409/2013) and that reporting on net fraud was already required as part of operational risk reporting under Basel II agreements.	The EBA is aware of the existing overlaps with the ECB Regulation on payment statistics and has for this reason been working in close cooperation with the ECB to ensure that the data required are consistent with the ECB Regulation where there is an overlap. The EBA and the ECB have also taken into account the outcome of the fact-finding exercise carried out by the ECB for a potential revision of the ECB Regulation. The proposed reporting under the Guidelines differs in some areas from the reporting required under the ECB Regulation on payment statistics and Basel II. This reflects the different rationales for reporting. The EBA also notes that the Guidelines no longer require the reporting of net fraud.	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
[187]	Double counting and double reporting	One respondent explained that, contrary to the EBA's argument that double counting can be avoided by not adding up figures, it is technically impossible for issuers and acquirers to distinguish those actions that have already been reported by other issuers or acquirers with reference to individual cases of fraud or individual fraudulent transactions. Some respondents argued that double counting and double reporting could not be avoided following the EBA's approach with respect to credit card payments and asked the EBA to explicitly exclude credit card acquirers from fraud reporting. One respondent further suggested that acquirers should deduct reports sent by issuers from their counting of fraud reporting, so that double reporting would be avoided in total. Without taking into account fraud reports by the issuer, the acquirer is obliged to report only frauds from sources other than the issuer, and double counting may be avoided.	PSPs should report all executed fraudulent transactions either from the issuer or from the acquirer or both. As these breakdowns will not be summed up, there is no need for the issuer to verify if the transaction was also reported by the acquirer and vice versa. Credit card acquirers are not excluded from the reporting.	*No change*
[188]	Double counting and double reporting	One respondent disagreed with the EBA that established branches could report separately to the host authority, given that often branches simply act as sales offices with centralised data processing at the home Member State PSP headquarters, particularly for multinational B2B customers. Separating fraud-related data would be very burdensome for PSPs with branches.	In line with the monitoring and reporting set out in Article 29(2) PSD2 and in Article 40 CRDIV for credit institutions, the established branch of an EEA's PSP should report to the CA of the host Member State where it is established, separately from the data of the PSP in the home Member State.	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		If, however, the EBA were to retain the concept of separate reporting through established branches, the respondent asked that the EBA clarify whether those fraudulent transactions that are reported by the branch to the host country CA should be deducted from the central reporting of the PSP to the home country CA.	The EBA believes that this option will ensure accurate information on the number of payment transactions and will not be excessively costly or difficult to apply. The EBA also confirms that data from established branches should be deducted from central reporting. The EBA notes, finally, that this is in line with current practice under the ECB Regulation on payment statistics.	
Feedback on responses to question 9				
[189]	Separating corporate from consumers' transactions	A number of respondents agreed with the EBA that an additional breakdown was not necessary, as the difference is not relevant for PSPs and would be difficult, thus increasing the reporting burden. In their view, the introduction of this additional distinction for all services and payment instruments identified by the EBA to the current reporting model would entail a heavy implementation cost that would outweigh the potential benefits. They also argued that such a distinction could not be accurately or consistently applied. In some cases, the distinction would be relatively straightforward, for example for cards, but for P2P platform payments, for example, the distinction could be more difficult. The requirement to break fraud data down on this basis would then be more onerous and give rise to inaccurate data.	The EBA agrees with the comments and maintains its view that an additional breakdown into consumer and corporate transactions would be overly complex and burdensome with limited added value. The EBA has therefore not introduced such an additional breakdown into the revised GL.	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
[190]	Separating corporate from consumers' transactions	Others disagreed with this view and thought that: - Such a breakdown is essential to understanding exactly where consumer detriment is taking place (avoiding misleading data). - Commercial card business reported under PSD2 should be split into personal and non-personal. - A separate commercial card reporting line for non-cardholder-linked products, such as virtual and lodge commercial card products, would be required. These products experience extremely low levels of fraud. - The difference in scope, frequency, average amount and purpose (statistically) between the payment transactions made by consumers and those made by other PSUs should lead to different monitoring criteria for payments made by consumers and those made by other PSUs. - There are differences between these services from liability and service perspectives. - Fraud methods are more sophisticated and targeted in relation to larger PSUs than in the consumer segment.	The EBA maintains its view that an additional breakdown into consumer and corporate transactions would be overly complex and burdensome with limited added value. The EBA has therefore not introduced such an additional breakdown into the revised GL.	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		In those respondents' view, such a distinction would help PSPs to better target their efforts on fraud prevention, and would fill a gap in the data that are currently monitored and reported. In addition, some respondents stated that the distinction might be helpful in the context of a potential new corporate exemption under the RTS on SCA and CSC.		
[191]	Separating corporate from consumers' transactions	Some respondents suggested adding data on the category of merchant involved in the transaction (where known) as an alternative, based on the merchant category codes already used for card-based and some digital wallet transactions, although possibly at a higher level and with fewer codes to facilitate reporting.	The proposal of using merchant category codes was considered. However, the EBA concluded that such an additional breakdown would be overly burdensome with limited added value and therefore should not be introduced.	*No change*
[192]	Separating corporate from consumers' transactions	Other respondents asked for clarification on what was meant by 'other PSUs'.	The EBA agrees that greater clarity would have been needed in this regard. 'Other PSUs' referred to corporate or business consumers.	*No change*
[193]	Separating corporate from consumers' transactions	A number of respondents disagreed with the suggestion by EBA that there had been reports of an increase in fraud figures at corporate level.	The EBA has noted the comment. It was decided that the additional breakdown was not required.	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
[194]	Separating corporate from consumers' transactions	Some respondents suggested defining corporate versus SME payment transactions, highlighting that these definitions might vary across Member States.	The suggestion that corporate versus SME payment transactions should be defined was considered. However, it was decided that the additional breakdown was not required.	*No change*
Other comments				
[195]	Other comments	One respondent expressed concern that the RTS on SCA and CSC do not provide for immediate legal recourse in a situation where an ASPSP (bank) has built and got approval for a dedicated API but this API, once approved, fails to deliver as expected.	This comment is not related to the EBA GL on fraud reporting and cannot therefore be addressed in this feedback table.	*No change*
[196]	Other comments	One respondent suggested that the EBA review its GL in the context of the Bank for International Settlements Committee on Payments and Market Infrastructures (CPMI) Methodology of the statistics on payments and financial market infrastructures in the CPMI countries, published in August 2017.	The EBA is of the view that the GL cannot be fully aligned with the CPMI methodology due to the following considerations: - Terminology: the EBA GL are secondary EU legislation and should be aligned with the terminology and definitions used in PSD2, Regulation (EU) 2015/751, Regulation (EU) No 260/2012 and Directive 2009/110/EC. - Geographical perspective: the EBA GL are intended to take an EU/EEA perspective while the CPMI methodology has a global perspective. In response to a number of comments by respondents, the EBA has further aligned the GL as far as possible with the methodology in the ECB Regulation on payment statistics, which also has some similarities with the CPMI	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
			methodology, thus also ensuring some alignment with the latter.	
[197]	Other comments	One respondent shared its view that Article 80(2) PSD2 should be complied with from 13 January 2018, given that fraud is measured by PISPs on the basis of the revocation of the payment order after the PSU has consented to the initiation.	Article 80(2) PSD2 has been applicable since 13 January 2018.	*No change*
[198]	Other comments	One respondent queried how transactions in branches should be reported (electronic or non-electronic). For instance, a customer may sign a form to consent for an electronic credit transfer to then be executed.	The EBA notes that PSD2 refers to electronic payment transactions. The GL cannot legally redefine terminology defined at Level 1.	*No change*
[199]	Other comments	Some respondents sought further guidance on how PSPs with multiple brands and product portfolios should report under the GL.	The general principles of PSD2 apply. No reporting by brands or product portfolio is envisaged.	*No change*
[200]	Other comments	A number of respondents sought further clarity on providing a breakdown of contactless and unattended terminals exemptions, authentication method and reason for authentication method.	The respondents did not explain precisely what clarifications they were seeking and the EBA was as a result unable to address the comment.	*No change*
[201]	Other comments	A number of respondents queried whether prepaid cards should be included in the reporting.	As specified in Guideline 7.2(b), prepaid card transactions are counted in e-money services.	*No change*
[202]	Other comments	Some respondents disagreed with the inclusion of reporting data outside the scope of PSD2, for example MOTO.	For statistical purposes, the GL require data on electronic and non-electronic transactions. However, the EBA agrees with the respondents to the extent that the detail	*Changes to the data breakdowns in Annex 2*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
			on non-electronic transactions is not necessary and the related material has been deleted from Annex 2.	
[203]	Other comments	Some respondents queried the use of the term 'payer's payment service provider' in the context of credit cards.	The EBA agrees that the reference may not be clear and has added references to card issuing and acquiring to the revised GL.	*Guideline 1.2:* For the purposes of **Guideline** ~~paragraph~~ 1.1 above, 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)**. Payment service providers should not report data on payment transactions **that** ~~which~~, however linked to any of the circumstances referred to in **Guideline** ~~paragraph~~ 1.1, have not been executed and have not **resulted in** ~~determined~~ a transfer of funds in accordance with PSD2 provisions. *Guideline 1.6.b:* For non-remote card-based payment transactions, 'domestic payment transaction' refers to a payment transaction where the **payer's payment service provider (**issuer**)**, **the payee's payment service provider (**acquirer**)** and the ~~location of the~~ point of sale (POS) or automated teller machine (ATM) used are located in the same Member State.
[204]	Other comments	A number of respondents asked for further clarification on several terms and definitions: – transactions initiated electronically; – remote and non-remote;	The terms referred to in the respondent's comment all originate from Level 1 regulations or directives and cannot legally be redefined in EBA GL. In addition as mentioned in comment 58 paper based and MOTO have been deleted from the guidelines.	*The sub-categories of MOTO and paper-based payments under non-electronic payment transactions have been removed from Annex 2*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
		– paper-based; – e-money; – MOTO transactions.		
[205]	Other comments	One respondent suggested combining all the separate tables into one flat structure to make it possible to slice and dice the data across the various dimensions.	The EBA has reached the view that a flat structure would probably be confusing for many PSPs and has therefore kept the different tables.	*No change*
[206]	Other comments	A few respondents expressed the view that the average ECB reference exchange rate was not available in the credit card processing data settings. They also argued that the use of average ECB reference exchange rate constituted a very broad approach to converting currencies.	The EBA agrees that this rate is not available for credit cards and has therefore added further text to Guideline 2.3, in line with the ECB regulations.	Guideline 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 in the non-euro area should report in the currency of that Member State. ~~They~~ **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 ~~either the official~~ **the** currency **they are supposed to report in** ~~of the Member State of establishment or the Euro currency~~, using **the relevant exchange rates applied to these transactions or** the average ECB reference exchange rate for the applicable reporting period.
[207]	Other comments	Some respondents expressed the view that the distinction between remote and non-remote was not relevant for credit transfers.	The EBA disagrees, on the basis that, in a number of European countries, customers can make credit transfers from an ATM. Such transactions would be considered non-remote. The EBA has concluded that this breakdown should therefore be included.	*No change*

Reference number	Response reference	Summary of responses received	EBA analysis and feedback	Amendments to the proposals
[208]	Other comments	Some respondents suggested that the use of SCA or non-SCA data should also include breakdowns by remote or non-remote and by channel.	The EBA has considered this suggestion and has clarified the cross-referencing of the data points by adding numbering to the breakdowns in Annex 2.	*Changes to cross-referencing in data breakdowns in Annex 2*
[209]	Other comments	If a transaction where the payee's PSP used the TRA exemption turns out to be fraudulent, the payer's PSP should not count that transaction in its fraud levels. By the same token, it should be clarified that, if it is the payer's PSP using the TRA exemption and the transaction turns out to be fraudulent, the payee's PSP's fraud levels should not be impacted.	The EBA is of the view that all fraudulent transactions should be reported. Section 3.2 of the Final Report also clarifies that, in the case of transactions processed by more than one PSP (e.g. card transactions), the fraudulent transactions included in the calculation for a given PSP's fraud rate should be based on (i) the unauthorised transactions for which the PSP has borne liability, as determined in accordance with Article 74 PSD2, and (ii) the fraudulent transactions that have not been prevented by the PSP.	*Clarification provided in paragraph 12 of section 3.2*
[210]	Other comments	A number of respondents recommended adding a reference to the GL to the way in which CAs will share in a timely manner with all PSPs in the market relevant information on the major incidents that small payment institutions and small e-money institutions have suffered.	The EBA is of the view that this is not relevant to the EBA GL on fraud reporting.	No change