EBA/CP/2017/13

02 August 2017

Consultation Paper

on Draft Guidelines on fraud reporting requirements under Article 96(6) of Directive (EU) 2015/2366 (PSD2)

Contents

1. Responding to this consultation

The EBA invites comments on all proposals put forward in this paper and in particular on the specific questions summarised in 6.2.

Comments are most helpful if they:

- respond to the question stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed/ rationale proposed; and
- describe any alternative regulatory choices the EBA should consider.

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 03.11.2017. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

Please clearly indicate in the consultation form if you wish your comments to be disclosed or to be treated as confidential. A confidential response may be requested from us in accordance with the EBA's rules on public access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by the EBA's Board of Appeal and the European Ombudsman.

Data protection

The protection of individuals with regard to the processing of personal data by the EBA is based on Regulation (EC) N° 45/2001 of the European Parliament and of the Council of 18 December 2000 as implemented by the EBA in its implementing rules adopted by its Management Board. Further information on data protection can be found under the Legal notice section of the EBA website.

2. Executive Summary

Directive (EU) 2015/2366 on payment services in the internal market (PSD2) entered into force in the European Union on 12 January 2016 and will apply as of 13 January 2018. One of the PSD2 requirements to all payment service providers relates to the reporting of fraud data on means of payment. More specifically, Article 96(6) PSD2 states that payment service providers (PSPs) shall provide "statistical data on fraud relating to different means of payment to their competent authorities". The same article states that the competent authorities shall, 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 is comparable and reliable, the EBA, in close cooperation with the ECB, is proposing two sets of Guidelines on the reporting requirements of fraudulent payment transactions. The first set of Guidelines sets out requirements applicable to all payment service providers, with the exception of account information service providers, while the second set of Guidelines sets out requirements that are applicable to all competent authorities.

More specifically, the first set of Guidelines defines "fraudulent payment transactions" for the purpose of the data reporting under these Guidelines, and set out the methodology for collating and reporting data, including data breakdown, reporting periods, frequency and reporting deadlines. Payment service providers are expected to provide high-level data on a quarterly basis and more detailed data on a yearly basis.

The level of data breakdown will depend on the payment instrument used or the payment service provided. The Guidelines leave it to the discretion of the competent authority to decide on the technological aspects of the reporting format and the means of communication.

The second set of Guidelines includes requirements for competent authorities on data aggregation and data reporting frequency and deadlines applicable to the EBA and the ECB.

These Guidelines apply from 13 January 2018.

Next steps

The consultation period will run from 02 August 2017 to 03 November 2017. The final Guidelines will be published after this consultation.

3. Abbreviations

AISP	Account Information Service Provider
CP	Consultation Paper
CSC	Common and Secure Communication
EBA	European Banking Authority
ECB	European Central Bank
EEA	European Economic Area
EMD	Electronic Money Directive
ESCB	European System of Central Banks
EU	European Union
GL	Guidelines
PISP	Payment Initiation Service Provider
PSD	Payment Services Directive
PSP	Payment Service Provider
PSU	Payment Service User
RTS	Regulatory Technical Standards
SCA	Strong Customer Authentication
TPP	Third Party Provider

4. Background and rationale

4.1 Background

1. Directive (EU) 2015/2366 on payment services in the internal market (PSD2) entered into force on 12 January 2016 and applies as of 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) of 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. Those competent authorities shall provide EBA and the ECB with such data in an aggregated form".

3. In order to ensure that these high-level provisions are implemented consistently across the Member States of the European Union (EU) and the European Economic Area (EEA), and to ensure that the aggregated data provided to the EBA and the ECB is comparable and reliable, the EBA, in close cooperation with the ECB, has developed two sets of draft Guidelines (GL) on fraud data reporting requirements. The first one is addressed to payment service providers (PSPs) while the second is addressed to competent authorities.

4. In what follows in the rationale section below, this Consultation Paper explains the reasoning for some of the options the EBA has considered and the decisions the EBA has taken during the development of the GL that are proposed in this Consultation Paper. This includes the objectives that the GL are aimed at achieving, the definition of fraudulent payment transaction, the addressees, the scope of the reporting requirements, the reporting of net vs. gross fraudulent payment transactions data, the frequency of reporting, the breakdown of data, double counting aspects and the consideration of the inclusion of an additional data breakdown between consumers and non-consumers.

4.2 Rationale

5. As highlighted in the EBA's Final Report on the draft Regulatory Technical Standards (RTS) on Strong Customer Authentication and Common and Secure Communication (SCA and CSC)[1], data on payment fraud in the EU is at present difficult to obtain, not reliable, and not comparable across Member States, therefore impeding the establishment of an accurate picture of payment fraud in the EU, including the understanding of its size, components and development over time.

6. Not all Member States 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, Member States that currently *do* collect fraud

[1] See https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf

either do not cover transactions with all payment instruments or transactions of all types of payment service providers within their jurisdiction, or the data categories and level of detail differs between them.

7. The European System of Central Banks (ESCB), in its function of overseer of payment schemes and instruments, collects fraud data, but that data is limited to card payments and based on non-legally binding reporting requirements. Additional payment statistics are collected by Central Banks in the subset of EU Member States that constitute the Euro area and covers data on all means of payment but does not, at the moment, cover reporting of data related to fraudulent payment transactions.[2]

8. The Guidelines proposed in this Consultation Paper are aimed at ensuring that comparable and reliable payment fraud data are reported to competent authorities across the EU and the EEA, which, in turn, will then send the aggregated data to the EBA and ECB. This will contribute to assessing the effectiveness of applicable legal and regulatory requirements aimed at reducing payment fraud, identifying fraud trends and potential risks across the EU and the EEA, assessing and comparing fraud data between different payment instruments, and inform any future regulatory and/or supervisory change or action. The collection of fraud data should also enable payment service providers to better assess security incidents or emerging fraud trends and threats.

9. In addition, several provisions of the PSD2, as well as some of the Technical Standards and GL developed by the EBA in support of the PSD2, such as the RTS on strong customer authentication (SCA) and common and secure communication (CSC) and the GL on operational and security risks, require payment service providers to monitor fraud data. More specifically, Article 17 of the RTS on SCA and CSC revised version[3] includes an exemption subject to defined reference fraud rates being met, which in turn requires standardisation of the collection of payment fraud data to be included in the calculation of the fraud rate, to ensure a level playing field across Member States and across the different PSPs.

10. Both the Guidelines on operational and security risks and the RTS on SCA and CSC are still in consultation, not yet finalised and may be subject to change before publication later in 2017. The EBA is of the view that the data requirement under the Guidelines proposed in this CP would enable PSPs to collect all data required to comply with Article 20 of the draft RTS revised version as well as for PSPs to monitor the use of the exemptions to SCA. Competent authorities, in turn, would be able to use the data gathered under these Guidelines to supervise and monitor the use of the exemptions to SCA and the fraud rates calculated by PSPs for the purpose of potential transaction risk analysis exemptions under the RTS on SCA and CSC.

11. These GL are divided into two sets: the first set of GL applies to PSPs and contains seven GL (GL 1 to 7) setting out requirements for data reporting from the PSP to the relevant competent

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

[3] Revised version as submitted by the EBA in conjunction with its Opinion on 29 June 2017, see http://www.eba.europa.eu/-/eba-publishes-its-opinion-in-response-to-the-european-commission-intention-to-amend-the-eba-technical-standards-for-open-and-secure-electronic-payment

authority which include detail on the fraudulent transactions data to be reported, the geographical breakdown, the frequency, methodology to follow, deadlines, etc.; and a second set that applies to competent authorities and contains three GL (GL 8 to 10) setting out the requirements for the reporting of the aggregate data from competent authorities to the EBA and the ECB. The first Guideline in each set of GL defines terminologies and applies to both competent authorities and PSPs.

12. The remaining part of the rationale provides detail on the following areas:

- the objectives of the GL;
- the definition of a fraudulent payment transaction for the purpose of providing statistical data under Article 96(6) PSD2;
- the addressees of the GL and the exclusion of Account Information Service Providers;
- the scope of the GL and the absence of reporting requirements of attempted fraud data;
- the inclusion of net vs. gross fraudulent payment transactions concepts;
- the frequency of reporting;
- the data breakdown;
- the risk of double counting and double reporting; and
- a possible further data breakdown distinguishing between consumers and other payment service users.

Objectives of the Guidelines

13. In the absence of any further details provided in the PSD2 itself as regards the specific aims of the provision in Article 96(6), the EBA and ECB started the development of these GL with the identification of the objectives that the GL are to achieve. The result of this assessment is depicted in the table below:

Party	Objectives
Competent authorities under PSD2 in their function as supervisors of payment service providers	- to provide a supervisory tool to understand whether there are market-wide or PSP- specific issues relating to fraud, its sources, and whether action needs to be taken as a result; - to check compliance with regulatory requirements, including with the EBA RTS on SCA and CSC, and assess whether the measures implemented by PSD2 itself and the security requirements that the EBA and ECB have developed in support of the Directive, are effective; - to inform any future revisions of security measures; - [potentially] to publish payments fraud reports and consumer education material.
ESCB in its function as overseer of payment systems and payment instruments	- to assist in its role to ensure the smooth operation of payment systems and the safety and efficiency of payment instruments by: o Having reliable data to assess security and efficiency of payments instruments and to evaluate the confidence of the users in the instruments and currency o Identifying fraud trends and analysing differences across payment instruments and Member States; - to inform any future revisions of security measures;

	- [potentially] to publish payments fraud reports.
EBA in its function as European supervisory authority	- to contribute to fulfilling its mandate to bring about regulatory and supervisory convergence across the EU Member States - to inform compliance across Member States with the security measures under PSD2 and secondary legislation, in particular the fraud threshold under the RTS on SCA and CSC; - to identify and compare differences between Member States in respect to fraud patterns, risks of potential consumer detriment; - to inform any future development of best practices where appropriate; - to inform any future revisions of security measures, in particular the statutory review of the RTS on SCA and CSC; - to understand over time whether specific existing measures have improved the security of payment transactions; - [potentially] to publish payments fraud reports and consumer educational material.
Payment service providers (PSPs)	- to compare own performance in preventing and mitigating fraud to country-level benchmark (if EBA/ECB or NCAs were to publish aggregated country-level data); - to collect transaction and fraud data as part of their risk monitoring and risk assessment, helping them to better assess security incidents and risks; - to pro-actively identify fraud trends for future risk identification and proactive mitigation; - to assist with monitoring compliance with requirements of RTS on SCA and CSC, and in particular with Articles 18 and 20 draft RTS.
Payment service users (PSUs)	- [If any aggregated data were to be published] to have access to regular, reliable and aggregated data about levels, sources and types of fraud at an EU and country-by-country level; - [In the event of data being used to release educational material] to learn about the risks of fraud, how to avoid it, and how to protect themselves and their sensitive payment data.

Question 1: Do you consider the objectives for the guidelines as chosen by the EBA, in close cooperation with the ECB, including the link with the RTS on SCA and CSC (and in particular Articles 18 and 20 RTS), to be appropriate and complete? If not, please provide your reasoning.

Definition of fraudulent payment transaction and data breakdowns

14. The next issue the EBA addressed was the definition of "fraud" that should be used as a basis for the GL, for reporting "fraud relating to different means of payment" as per Article 96 (6) PSD2. Across the PSD2, provisions and recitals make various references to payment fraud-related terms, such as "unauthorised or fraudulent use of the payment instrument", "unauthorised or fraudulent initiation of a payment transaction", "payer acting fraudulently" or "fraud relating to different means of payment".

15. However, no definition of payment fraud is provided that the EBA and ECB could use as a basis to fulfil the mandate. As a result, the GL proposed in this CP define the term "fraud" such that it is understood as "fraudulent payment transactions" for the specific purpose of statistical data reporting under Article 96(6).

16. According to this definition, “fraudulent payment transactions” includes all instances of payment fraud that occur in the payment market, including not only unauthorised payment transactions but also transactions where the payer was manipulated, or where the payer acted fraudulently.

17. Moreover, the proposed GL determine breakdowns for “fraudulent payment transactions” to be reported and does so without making use of terms such as “phishing”, “social engineering” or similar. This is due to the wide variety of interpretations of these non-technologically neutral terms across market participants, the different techniques for performing the same fraudulent payment transaction, as well as the absence of direct connection with the source of credentials for authorisation.

18. Instead, the GL therefore categorise fraud in a more technology-neutral way, the different breakdowns of which are provided in Annexes 2 and 3. They do so by looking at (a) the location where the fraud takes place in the payment chain; (b) the authentication method that failed to prevent the fraudulent payment; (c) the payment channel in which the transaction took place, and (d) the way in which the fraudster gained access to the sensitive payment data.

19. The EBA acknowledges that the payment market, as well as fraud more generally, may evolve rapidly, which may require new categories to be added in the future, which would then be subject to a review and re-consultation.

Question 2: In your view, does the definition of fraudulent payment transactions (in Guideline 1) and the different data breakdown tables (in Annexes 2 and 3) cover all relevant statistical data on “fraud on means of payment” that should be reported? If not, please provide your reasoning with details and examples of which categories should be added to, or existing categories modified in, the Guidelines.

Addressees of the Guidelines

20. Given the focus of Article 96 PSD2 on “fraud relating to different means of payment”, it is EBA’s interpretation that all payment service providers that are part of a payment transaction chain should be in scope of the reporting requirements under these GL.

21. The EBA is also of the view that fraud data from those PSPs that provide only account information services may be redundant and cause double counting issues given that any fraud that may have its origin in a data breach from an account information service provider will be recorded by the PSP executing the payment transaction where the stolen or inappropriately obtained data will be used.

22. The EBA has therefore arrived at the view that those PSPs that provide account information services only should be excluded from the requirements of these GL as they do not execute payment transactions and therefore could not report in any way “fraudulent payment transactions”. The EBA however encourages those PSPs to monitor and manage fraud related to their business and the risks it causes to the payment service users.

23. The EBA also takes comfort from the fact that those PSPs that provide account information services only are not otherwise exempt from regulation. They are, for instance, subject to all security requirements under PSD2 and related legal instruments issued by the EBA, such as the EBA GL on major incident reporting, the GL on operational and security risks and, of course, the EBA RTS on SCA&CSC.

Question 3: Do you agree with the EBA's proposal to exempt Account Information Service Providers from reporting any data for the purpose of these Guidelines? Please provide your reasoning with detail and examples.

Scope of reporting requirements

24. Under Article 4(5) PSD2, "'payment transaction' means an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee".

25. Given this definition, the EBA has considered whether it should also include *attempts* to carry out fraudulent payment transactions in the data reporting. Capturing data on such fraud attempts would enable competent authorities to assess the effectiveness of the internal controls of the PSP in blocking transactions before they are executed.

26. However, including such fraudulent transactions attempts would also substantially increase the amount of data to be collected and submitted by each provider, as well as the data to be aggregated by competent authorities. It is also likely to complicate the analysis of the data received.

27. Under the EBA's RTS on SCA and CSC, all PSPs shall have risk and fraud monitoring systems in place to enable them to block any suspicious payment as foreseen by PSD2. The EBA would therefore expect payment service providers to monitor the effectiveness of their systems, including by measuring the number of fraudulent transaction attempts blocked in an effective manner.

28. The EBA has therefore arrived at the view that, on balance, Guideline 2.5 should not require payment service providers to provide any data with regard to attempted fraud.

Question 4: Do you agree with the rationale for not including in Guideline 2.5 a requirement to report data for attempted fraud for the purpose of these Guidelines? If not, please provide your reasoning with detail and examples.

Net and gross fraudulent payment transactions data

29. It is essential for regulatory authorities to be able to monitor and analyse data on fraudulent payment transactions for the purpose of consumer protection, and maintaining the integrity of the EU payment market and require the reporting of gross figures of all fraud that has been recorded. However, the EBA is of the view that it is equally important to report in addition net

figures for the same reporting period to enable competent authorities to identify to which extent the financial damage has been recovered by the reporting entity and where the liability for the payment fraud may lie.

30. The EBA equally recognises that any given payment service provider would not be able to measure, and at times may even not be aware of the net figure, i.e. the figure reflecting the scenario where the fraud loss may have been recovered by another party in the payment transaction chain and/or from the fraudster himself.

31. The EBA has therefore arrived at the view, as specified in Guideline 1, and Guideline 1.5 in particular, that it would be appropriate for PSPs to report both net and gross fraud, with net figures only taking into account losses that have been recovered by the reporting payment service provider (rather than by all actors in the payment chain) from any source including an insurance company, a party in the payment chain such as the payee's PSP, or if the loss has eventually been recovered from the fraudster himself.

Question 5: Do you agree with the proposal for payment service providers to report both gross and net fraudulent payment transactions, with net fraudulent transactions only taking into account funds recovered by the reporting institution (rather than any other institution) as set out in Guideline 1.5? If not, please provide your reasoning with detail and examples.

Start date and frequency of reporting

32. Article 96(6) PSD2 requires the reporting to be "at least on an annual basis", which allows for the possibility of a more frequent reporting. The EBA considered various options in respect of the specific frequency through which reporting should take place. To that end, the EBA considered that, in line with the objectives of the GL set out at the beginning of the rationale section, fraud data will be used as a tool for supervisory authorities to have information on fraudulent payment transactions so as to be able to take supervisory or regulatory action where needed.

33. The EBA is therefore of the view that, for competent authorities to be able to act promptly, some fraudulent payment transactions data need to be reported more frequently than on an annual basis, so that sources of fraud can be timely detected and mitigated and potential detriment to customers, providers and the payments system more generally adequately reduced or prevented.

34. The EBA is also of the view that more frequent reporting improves the quality of the data and notes that this is in line with reporting for ESCB's fraudulent card-based payment transactions oversight reporting obligations to a number of payment schemes. Given that some competent authorities currently receive statistical reports on a monthly basis whilst others report on an annual basis, the EBA is of the view that providing some high level fraudulent payment transactions data on a quarterly basis is proportionate, necessary and a suitable compromise.

35. Eventually, the EBA arrived at the view that the GL should require detailed data to be reported as set out in Guideline 3 and specified further in Annex 2 on an annual basis and, in addition, less detailed data to be reported under Annex 3 on a quarterly basis.

36. Furthermore, Guideline 3.2 states that smaller payment service providers that benefit from an exemption under Article 32 PSD2 or Article 9 Electronic Money Directive (EMD) are not required to report any data on a quarterly basis and should only report the data required on an annual basis.

37. Finally, based on the frequency described above, the EBA is of the view that PSPs should report fraudulent payment transactions from the moment the fraud has been reported to, or discovered by, the PSP rather than wait until the fraud case has been closed. This means that the fraud data collected at any stage may include potential fraud, which may not yet have been confirmed and that the data may require some adjustments at a later stage and as foreseen under the GL.

38. The proposed GL apply from 13 January 2018, which means that PSPs will be required to record fraudulent transactions from that day onwards. The reporting of that data, by contrast, will take place at later stage and will also vary in detail. For high level data to be reported on a quarterly basis as specified in Annex 3, the first reporting will take place in 2018H2 and cover payment transactions and fraudulent payment transactions that occurred during 2018Q2, as the first full quarterly period. Detailed data as specified in Annex 2 of the GL will be reported annually. The first reporting period will take place in 2020H1 covering transactions and fraudulent transactions that occurred from the date of application of the RTS on SCA and CSC as specified in Article 115(4) PSD2.

Question 6: Do you consider the frequency of reporting proposed in Guideline 3, including the exemption from quarterly reporting for small payment institutions and small e-money institutions in light of the amount of data requested in Annexes 1, 2 and 3, to be achieving an appropriate balance between the competing demands of ensuring timeliness to reduce fraud and imposing a proportionate reporting burden on PSPs? If not, please provide your reasoning with detail and examples.

Breakdown of data

39. The EBA considers it essential for the statistical data to be comprehensive in order to provide as complete a picture of fraudulent payment transactions as possible. However, the EBA also considered the need for proportionality so that the reporting requirements would not be overly burdensome. The EBA therefore identified and assessed the data that the different types of payment service providers could be required to report and at which level of detail this should be done, depending on the type of payment service they provide and the payment instrument used.

40. These considerations have led to the development of Guideline 7 and the breakdowns detailed in Annexes 2 and 3. The two annexes distinguish between e-money issuance, payment initiation

services, money remittance and all other payment services, depending on whether they are performed by means of a direct debit, credit transfer or card-based payment instrument.

41. More specifically, each annex includes seven separate data requirements with breakdowns for all payment service providers depending on the type of payment service or the type of payment instrument for which the fraud occurred:

    - Data breakdown A/E for e-money services,
    - Data breakdown B/F for money remittance services,
    - Data breakdown C/G for payment initiation services,
    - Data breakdown D1/H1 for credit transfers,
    - Data breakdown D2/H2 for direct debit services,
    - Data breakdown D3/H3 for payment cards issuance,
    - Data breakdown D4/H4 for payment cards acquiring.

42. Payment service providers may need to provide data for more than one payment instrument or payment service depending on their activities. Annex 2 details more granular data requirements to be provided on an annual basis, while Annex 3 details more high-level data requirements to be provided on a quarterly basis. Annex 1 details general data requirements applicable to all reporting data breakdown, including data on the PSP and geographical breakdown. Payment service providers must always provide statistical data in value and volume, for both fraudulent payment transactions and total payment transactions.

Question 7: Do you agree that payment service providers will be able to report the data specified in Guideline 7 and each of the three Annexes? If not, what obstacles do you see and how could these obstacles be overcome?

Double counting and double reporting

43. The EBA has largely avoided any risk of double reporting by applying to the development of the GL the principle that only one provider, the sender or receiver of the transaction funds, reports the underlying payment transaction.

44. However, the EBA is also of the view that, in order for competent authorities to be in a position to obtain a comprehensive view of fraudulent transactions in card-payments, the PSP of both, the payer and the payee should report data. This will prevent having only a partial view on any fraudulent payment flow and thus would allow covering potential fraudulent cases on the payee's side that are not known to or cannot be controlled by the payer's PSP. The EBA acknowledges that this requirement will result in the double reporting of the same transaction by two payment service providers but is of the view that not doing so would impede the ability for competent authorities comprehensively to capture and identify the origin, source and destination of fraudulent payment transactions.

45. In addition, double reporting would only lead to misrepresentation and miscalculation if it led to double counting, i.e. counting the same fraudulent payment transaction twice, for instance as a result of it being reported both by the payer's and the payee's PSP (i.e. issuing and acquiring). The EBA is of the view that the risk of double counting can be avoided by *not* adding up the number or value of card payment transactions from the payer's side to the number or value of the same transactions from the payee's side when reporting to the competent authority.

46. The situation is the same with regards to the requirement for reporting a payment transaction both by the payment service provider that executed the transaction and the payment initiation service provider that initiated the payment transaction. However, similarly to the situation above, the EBA is of the view that the number or value of transactions that are recorded under different headings should not be summed up, eliminating the risk of double counting.

47. Despite the fact that the EBA has identified the scenarios of double reporting and double counting that are most relevant, the EBA acknowledges that there might be a residual issue of double counting and double reporting but that the frequency and likelihood of any such scenario would be limited and is therefore acceptable.

Question 8: In your view, do the proposed Guidelines reach an acceptable compromise between the competing demands of receiving comprehensive data and reducing double counting and double reporting? If not, please provide your reasoning.

Data breakdown between consumers and other payment service users

48. The EBA has been made aware via the different security fora of the payments market of increasing fraud figures and trends at corporate level (at times referred to as 'CEO fraud') and considers it important to monitor such developments. The EBA considered whether an additional data breakdown distinguishing between payment transactions or fraudulent payment transactions made by a consumer on the one hand and other payment service users (PSUs), such as businesses, on the other should be introduced. This requirement would apply irrespective of whether or not the RTS on SCA&CSC, which is currently in the process of being adopted by the EU Commission, will contain an exemption on certain types of corporate payments.

49. The EBA understands that payment service providers may not always be able to distinguish between consumers and other types of PSUs and has as a result at present not included such data breakdown.

50. The EBA would like to hear the views of market participants about any reasons that may prevent PSPs to make such a differentiation, and how these obstacles could be overcome.

Question 9: Are you of the view that payment services providers should distinguish between payment transactions made by consumers and payment transactions made by other PSUs? Please provide your reasoning with detail and examples.

5. Draft Guidelines

EBA/GL-REC/20XX/XX

DD Month YYYY

Draft Guidelines

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

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[4]. 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 the EBA 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 as to whether they comply or intend to comply with these guidelines, or otherwise with 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/2017/xx'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities. Any change in the status of compliance must also be reported to EBA.

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

[4] 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 services providers have to report to their competent authorities, as well as the aggregated data that the competent authorities have to share with the EBA and the ECB, under Article 96(6) of Directive (EU) 2015/2366 (PSD2).

Scope of application

6. These guidelines apply in relation to the reporting to competent authorities of statistical data on fraud by reference to fraudulent payment transactions data over a defined period of time as well as the total payment transactions over that period, by payment service providers for the payment transactions that they initiate and/or execute.

7. Payment transactions initiated by a resident PSP and executed without a specific transaction order, i.e. without the use of a payment service, by simple book entry on the account of a non-monetary financial institution, are not included.

8. Data reported under the form of credit transfers should include credit transfers performed via ATMs 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.

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

10. Data reported under card payments forms should include data on card transactions at virtual points of sale, e.g. over the internet. Card payments with cards issued by resident PSPs which only have an e-money function should not be included in card payments but reported as e-money. In line with PSD2 and the scope of application of strong customer authentication, payment service providers shall only report data breakdown on strong customer authentication and the use of any exemptions under the RTS on strong customer authentication and common and secure communication for payment transactions within the European Economic Area; payment transactions that have one leg outside of the EEA shall not be reported in the context of the use, or exemption thereof, of strong customer authentication.

11. These guidelines also apply to the aggregation of the data mentioned in paragraph 5 that competent authorities shall provide to the ECB and the EBA according to Article 96(6) PSD2.

12. 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 frequency of reporting, may differ between payment service providers, depending on their size, business model and complexity of their activities.

Addressees

13. These guidelines are addressed to:

    a. 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) 1093/2010 and to

    b. competent authorities as defined in point (i) of Article 4(2) of Regulation (EU) 1093/2010.

Definitions

14. Unless otherwise specified, terms used and defined in Regulation (EU) 2015/751 of the European Parliament council of 29 April 2015 on interchange fees for card-based payment transactions Directive and (EU) 2015/2366 of 25 November 2015 on payment services in the internal market have the same meaning in these Guidelines.

Date of application

15. These guidelines apply from 13 January 2018.

3. Guidelines on fraud data reporting applicable to Payment Service Providers

Guideline 1: General and Fraudulent Payment Transactions

1.1. For the purposes of reporting statistical data on fraud according to the data breakdowns in Guideline 7 and Annexes 2 and 3, the payment services 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;

b. 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;

c. payment transactions made as a result of the payer being manipulated.

1.2. For the purposes of paragraph 1.1 above, the payment services provider should report only payment transactions that have been initiated and executed. Payment service providers should not report data on payment transactions which, however linked to any of the circumstances referred to in paragraph 1.1, have not been executed and have not determined 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, it is the payer's payment services 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 transactions should not be reported by the payment service provider of the beneficiary.

1.4. The transactions and fraudulent transactions where funds have been transferred by a money remitter payment service provider from its accounts to a beneficiary account should be reported by the money remitter payment service provider via the forms B/F. These transactions should not be reported by the payment service provider of the beneficiary.

1.5. The transactions and fraudulent transactions where e-money have been transferred by an e-money provider to a beneficiary account, including the case where the payer's PSP is identical to the payee's payment service provider, should be reported by the emoney provider using data breakdown A/E. Where the PSPs are distinct, payment is only reported by the payer's PSP to avoid double counting.

1.6. Payment services provider 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 (also called "national") payment transactions' refer to payment transactions initiated by a payer, or by or through a payee, where the payer's payment service provider that holds the payer's payment account and the payee's payment service provider that holds the payee's payment account are located in the same Member State.

b. For non-remote card-based payment transactions, a 'domestic payment transaction' refers to a payment transaction 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. If the issuer and the acquirer are in different Member States or the payment instrument is issued by an issuer located in a Member State different from that of the point of sale, the transaction is 'EEA cross border payment transaction';

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

d. 'EEA cross-border payment transactions' refer to a payment transaction initiated by a payer, or by or through a payee, where the payer's payment service provider who holds the payment account and the payee's payment service provider holding the payee's payment account are located in different Member States;

e. 'Cross-border payment transactions 1 leg outside EEA' refer to a payment transaction initiated by a payer, or by or through a payee, where either the payer's or the payee's payment service provider who holds the payment account is located outside the EEA while the other is located within the EEA;

f. 'Total gross 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. 'Total net fraudulent payment transactions' refer to the total of gross fraudulent payment transactions as referred to in guideline 1.6(f) minus the amount of fraudulent payment transactions that has been recovered by the reporting PSP from any source including an insurance company, a party of the payment chain such as the payee's PSP, or if the loss has eventually been recovered from the fraudster himself.

h. 'Manipulation of the payer' refers to where the payer issues a payment order, or gives the instruction to do so to the payment service provider, in good-faith, to the fraudster as a beneficiary (e.g. the fraudster impersonates a payee to which the payer consents to transfer money to);

i. 'Modification of a payment order by the fraudster' refers to 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;

j. 'Issuance of a payment order by the fraudster' refers to 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 forms under Annexes 2 and 3;

b. total fraudulent payment transactions, as well as

c. any data breakdown required in these Guidelines for these two aggregates.

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

2.3. A payment services 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 should convert data for values of transactions or fraudulent transactions denominated in a currency other than the Member State's official currency into either the official currency of the Member State of establishment or the Euro currency, using the average ECB reference exchange rate for the applicable reporting period.

2.4. The payment services provider should report fraudulent payment transactions data both on a gross and on a net basis as understood and defined in guidelines 1.6(f) and 1.6(g).

2.5. The payment services provider should report only payment transactions that have been executed. Attempted fraudulent transactions that are suspected for fraud and blocked before they are executed should not be included.

2.6. The payment services provider should report the statistical information with a breakdown in accordance with the forms specified in these Guidelines and compiled in Annexes 2 and 3.

2.7. The payment service providers should identify the applicable data breakdown(s), depending on the service(s) and payment instrument(s) provided, and submit the

applicable data to the competent authority following the procedures defined by the competent authority.

2.8. The payment service provider should be recording and reporting on an annual basis using the data breakdown(s) set out in Annex 2 of these Guidelines, and should be recording and reporting on a quarterly basis using the data breakdown(s) set out in Annex 3.

2.9. The payment service provider should ensure that all data reported to the competent authority can be cross-referenced and linked in line with the format provided by the competent authority. To that end, all data dimensions contained as tables in annexes 2 and 3 within the same section need to be concurrently supported by a reported data series upon request of the competent authority.

2.10. The payment service provider should allocate each transaction to only one sub-category in each table. As the sub-categories are mutually exclusive, the total (volume or value) of payment transactions and fraudulent payment transactions in the category is the sum of the sub-categories.

2.11. 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 counting as one.

2.12. 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 field and breakdown because that particular data breakdown is not applicable to that PSP, the data should be reported as “NA”, with an explanatory note explaining the reason for it not being applicable.

2.13. When reporting direct debit transactions, the payment service provider should deduct the transactions rejected or recalled from the total reported.

2.14. For the purpose of avoiding double-counting as much as possible and maintaining the quality of the data, the payment service provider should submit data in their capacity as the sending participant in a transaction. As an exception, for card payments, data should be 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 payee’s payment service provider (i.e. counted on the acquiring side in the country in which the transaction is received). The two perspectives should be reported separately, with different forms as detailed in Annexes 2 and 3 respectively.

2.15. The direction of flow of funds depends on the payment service and payment instrument used:

a. In the case of credit transfers and similar transactions where the payer initiates the transaction, the sending participant is also the sender of funds. Data should be reported solely by the payer’s PSP;

b. In the case of direct debit payment transactions and similar transactions, transactions where the payee initiates the transaction and the sending participant is the recipient of funds should be reported solely by the payee's PSP; and

c. In the case of card-based transactions, although the payee initiates the transaction, for the purpose of these guidelines the sending participant is also the sender of funds and the receiving participant is the recipient of funds. For the purpose of having an overall view of fraud types and sources both the payee's payment service provider and the payer's payment service provider should be recording and reporting data, albeit separately via different forms in order to avoid double-counting.

2.16. The payment services provider that executes payment transactions initiated by Payment Initiation Service Providers should indicate the volume and value of the total transactions that have been initiated by a Payment Initiation Service Provider to facilitate the identification by competent authorities of payment transactions that should also be reported by payment initiation service providers.

Guideline 3: Frequency and reporting timelines

3.1. The payment services provider should report data 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.

3.2. The payment services provider 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 (EMD) should only report the full set of data requested under the applicable form(s) under Annex 1 on an annual basis.

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

Guideline 4: Geographical breakdown

4.1 Payment services 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.

Guideline 5: Reporting to competent authority

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

5.2. 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 payment service provider should report to the competent authority of the host Member State where it is established, separately from the data of the PSP in the home Member State.

5.3. The payment service provider should record data from all their agents, where applicable, providing payment services in the EEA and aggregate these data with the rest of their own data before reporting to their home competent authority.

5.4. When reporting data to the corresponding competent authority, the payment service provider should make mention at a minimum of the details of identification of the provider mentioned in Annexes 1 to 3.

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 Payment service providers 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 is reported.

6.3 Payment service providers should report all adjustments to the data referring to any past reporting period at least up to a year old during the next reporting window after the information necessitating the adjustments is discovered. They should indicate that the data reported is a revised figure applicable for the past period according to the methodology established by the respective competent authority.

Guideline 7: Data breakdown

7.1 For e-money transactions as defined in Directive 2009/110/EC, the payment service provider should provide data in accordance with Data Breakdown A in Annex 2 and Data Breakdown E in Annex 3.

7.2 When providing data on e-money transactions, the payment services 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 is used.

7.3 The payment service provider for the purpose of 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 under Chapter 3 of the Regulatory Technical Standards on Strong customer authentication and common and secure communication EBA/RTS/2017-02), and

e. Fraud types.

7.4 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.

7.5 For money remittance services, the payment service provider should provide data in accordance with Data Breakdown B in Annex 2 and Data Breakdown F in Annex 3 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 geographical breakdown.

7.6 When providing payment initiation services, the payment service provider should provide data in accordance with Data Breakdown C 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.

7.7 For those payment transactions that qualify under Data Breakdown C in Annex 2 and G in Annex 3, PSPs offering payment initiation services should record and report data on volumes and values with the following breakdowns:

a. Geographical,

b. Payment instrument,

c. Payment channel, and

d. Authentication method.

7.8 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.

7.9 The payment service provider offering credit transfer and card payment based services should provide data included in Data Breakdown D1, D3 and D4 in Annex 2 and Data Breakdown H1, H3 and H4 in Annex 3, depending on the payment instrument used for a given payment transaction as well as the role of the payment service provider. The data include:

a. Geographical breakdown,

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, and

f. Payment transactions initiated via a payment initiation service provider.

7.10 For the purpose of quarterly reporting the payment service provider is not required to provide the data listed under points c), d) and e).

7.11 The payment services provider should provide data included in Data Breakdown 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.

7.12 The payment services provider should provide data included in Data Breakdown 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 side where a card was used and the payment service provider was the payer's payment service provider.

7.13 The payment services provider should provide data included in Data Breakdown D4 in Annex 2 for annual reporting and Data Breakdown H4 in Annex 3 for quarterly reporting for all payment transactions on the receiving side where a card was used and the payment service provider is the payee's payment service provider.

7.14 The payment services provider should provide data in Data Breakdown D2 in Annex 2 for annual reporting and Data 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 payment based services.

4. Guidelines on fraud data reporting applicable to Competent Authorities

Guideline 8: Fraudulent Payment Transaction

8.1. The competent authority should ensure that for the purposes of reporting statistical data on fraud according to the data breakdowns in Guideline 7 and Annexes 2 and 3, 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;

b. 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;

c. payment transactions made as a result of the payer being manipulated.

8.2. For the purposes of Guideline 8.1 above, the competent authority should report only payment transactions that have been initiated and executed. The competent authority should not report data on payment transactions which, however linked to any of the circumstances referred to in paragraph 8.1, have not been executed and have not determined a transfer of funds in accordance with PSD2 provisions.

8.3. 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 (also called "national") payment transactions' refer to payment transactions initiated by a payer, or by or through a payee, where the payer's payment service provider who holds the payer's payment account and the payee's payment service provider who holds the payee's payment account 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. 'EEA cross-border payment transactions' refer 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 who holds the payer's and payee's payment account respectively are located in different Member States;

d. 'Cross-border payment transactions 1 leg outside EEA' refer to a payment transaction initiated by a payer, or by or through a payee, where either the payer's or the payee's payment service provider who holds the payer's and payee's payment account respectively is located outside the EEA while the other is located within the EEA;

e. For non-remote card-based payment transactions, a 'domestic payment transaction' refers to a payment transaction 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. If the issuer and the acquirer are in different Member States or the payment instrument is issued by an issuer located in a Member State different from that of the point of sale, the transaction is 'EEA cross border payment transaction';

f. 'Total gross 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. 'Total net fraudulent payment transactions' refer to the total of gross fraudulent payment transactions as referred to in guideline 8.3(f) minus the amount of fraudulent payment transactions that has been recovered by the reporting PSP from any source including an insurance company, a party of the payment chain such as the payee's PSP, or if the loss has eventually been recovered from the fraudster himself.

h. 'Manipulation of the payer' refers to where the payer issues a payment order, or gives the instruction to do so to the payment service provider, in good-faith, to the fraudster as a beneficiary (e.g. the fraudster impersonates a payee to which the payer consents to transfer money to);

i. 'Modification of a payment order by the fraudster' refers to 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;

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

Guideline 9: Data collection and aggregation

9.1. The competent authority should report statistical information on:

a. total payment transactions in line with the different data breakdowns under Annexes 2 and 3;

b. total fraudulent payment transactions, as well as

c. any further data breakdown required in these Guidelines for these two aggregates.

9.2. The competent authority should report the statistical information in Guideline 9.1 in terms of both volume (i.e. number of transactions or fraudulent transactions) and value (amount of transactions or fraudulent transactions). They should report volumes and values in actual units, with two decimals for values.

9.3. The competent authority in a Member State of the Euro-area should report the values in Euro currency, whereas the competent authorities of in a Member State in the non-Euro area should report in the currency of that Member State. They should convert data for values of transactions or fraudulent transactions denominated in a currency other than the Member State's official currency into either the official currency of the Member State of establishment or the Euro currency, using the average ECB reference exchange rate for the applicable reporting period.

9.4. The competent authority should report fraudulent payment transactions data both on a gross and on a net basis as understood and defined in guidelines 8.3(f) and 8.3(g).

9.5. 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.

9.6. The competent authority should aggregate the data collected within their Member State from the addressees of this Guideline by summing up the figures reported for each individual payment service provider in line with the data breakdowns specified in Annexes 1 and 2. The competent authority should be recording and reporting aggregate data on an annual basis using the data breakdowns set out in Annex 2 of these Guidelines, and should be recording and reporting on a quarterly basis using the data breakdowns set out in Annex 3.

9.7. The competent authority should at all times preserve the confidentiality and integrity of the information exchanged and their proper identification when submitting data to the ECB and the EBA.

9.8. The competent authority should define the secure communication procedures and format for the reporting of the data by the payment services providers. The competent authority should also ensure that an adequate cut-off time is provided for payment service providers to ensure the quality of the data and to account for the potential delay in reporting fraudulent payment transactions.

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

9.10. The competent authority should at a minimum ensure that the data reported under these Guidelines can be cross-referenced and used by the EBA and the ECB according to any

potential combination of data characteristics to be prescribed by the competent authority for the purpose of the reporting of the payment service providers within the member state of the competent authority.

Guideline 10: Data reporting

10.1. The competent authority should aggregate data from each payment service provider and established branches received at the Member State level and then submit the aggregated data to the EBA and the ECB following the same categories, breakdown and principles as detailed under Guidelines 1.3 to 1.5 and Guideline 7.

10.2. The competent authority should report the values of payment transactions and fraudulent payment transactions in line with Guidelines 9.1 and 9.2. In order to avoid double counting, data should not be aggregated across different payment service categories.

10.3. The competent authority should report adjustments for any past reporting periods for any fraudulent payment transaction dated up to 13 months old during the next reporting window after the information necessitating the adjustments is discovered, by submitting revised data with an explanatory note and within three years.

10.4. The competent authority should send the aggregated data to the ECB and the EBA within six months starting the day after the end of the reporting period for both quarterly and yearly reporting.

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

10.6. The competent authority should agree with the ECB and, separately or jointly, with the EBA, the secure communication procedures and specific format in which the competent authorities should report the data.

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

The data required below are applicable to all reporting PSPs and data breakdown specified under Annexes 2 and 3.

General data on the reporting PSP

PSP Name: full name of the PSP subject to the data reporting procedure as it appears in the applicable official national PSP registry.

PSP unique identification number: the relevant unique identification number used in each Member State to identify the PSP, when applicable.

PSP authorisation number: Home Member State authorisation number, when applicable.

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

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

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

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

Geographical data breakdown

	Value and volume
Geo 1	Domestic; Cross-border within the EEA
Geo 2	Domestic; Cross-border within the EEA; Cross-border 1 leg outside EEA
Geo 3	Domestic; Cross-border within the EEA; Cross-border 1 leg outside EEA; Single country breakdowns – all EEA countries

Annex 2 – Annual Data Reporting Requirements for PSPs

The first reporting period should take place in 2020H1 covering transactions and fraudulent transactions that occurred from the date of application of the RTS on SCA and CSC as specified in Article 115(4) PSD2.

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

Payment service providers should provide data for both, all payment transactions and the subset of all fraudulent payment transactions, except for Table 5, which is applicable only to fraudulent payment transactions.

Table 1. Total transactions and fraudulent transactions

	Volume	Value
Total Payment Transactions	Geo 3	Geo 3
Total Gross Fraudulent Payment Transactions	Geo 3	Geo 3
Total Net Fraudulent Payment Transactions	Geo 2	Geo 2

Table 2. Data breakdown - payment channel

	Volume	Value
Remote	Geo 3	Geo 3
Non-remote	Geo 3	Geo 3

Table 3. Data breakdown - authentication method

	Volume	Value
SCA	Geo 2	Geo 2
Non-SCA	Geo 2	Geo 2

Table 4. Data breakdown - reason for authentication choice

Table 4.1. Reason for authentication via SCA

	Volume	Value
Increased risk of fraud based on trans. Monitoring outcome as per Art. 18 (5) RTS	Geo 1	Geo 1
Not eligible for exemption as per Art. 18 (1) RTS	Geo 1	Geo 1

Other	Geo 1	Geo 1

Table 4.2. Reason for authentication via non-SCA

Table 4.2.1 For remote payment channel

	Volume	Value
Low value	Geo 1	Geo 1
TRA	Geo 1	Geo 1
Trusted beneficiary	Geo 1	Geo 1
Recurring transaction	Geo 1	Geo 1

Table 4.2.1.a Transaction intervals (only with reference to TRA reason for authentication)

	Volume	Value
<100 €	Geo 1	Geo 1
≥100 and <250	Geo 1	Geo 1
≥250 and <500	Geo 1	Geo 1
≥500	Geo 1	Geo 1
	Geo 1	Geo 1

Table 4.2.2 For non-remote payment channel

	Volume	Value
Contactless low value	Geo 1	Geo 1
Unattended terminal for transport or parking fares	Geo 1	Geo 1

Table 5. Fraud types

	Volume	Value
Issuance of a payment order by the fraudster (incl. account takeover)	Geo 2	Geo 2
Modification of a payment order by the fraudster	Geo 2	Geo 2
Manipulation of the payer	Geo 2	Geo 2
Payer acted fraudulently	Geo 2	Geo 2

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

For all tables, payment service providers should provide data both for all payment transactions as well as for all fraudulent payment transactions.

Table 1. Total transactions and fraudulent transactions

	Volume	Value
Total Payment Transactions	Geo 3	Geo 3
Total Gross Fraudulent Payment Transactions	Geo 3	Geo 3
Total Net Fraudulent Payment Transactions	Geo 2	Geo 2

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

For all tables, payment service providers should provide data both for all payment transactions as well as for all fraudulent payment transactions.

Table 1. Total transactions and fraudulent transactions

	Volume	Value
Total Payment Transactions	Geo 3	Geo 3
Total Gross Fraudulent Payment Transactions	Geo 3	Geo 3
Total Net Fraudulent Payment Transactions	Geo 2	Geo 2

Table 2 – Data breakdown – payment instrument

	Volume	**Value**
Credit transfers	Geo 3	Geo 3
Direct debits	Geo 3	Geo 3
Card payments	Geo 3	Geo 3
Emoney	Geo 3	Geo 3

Table 3. Data breakdown – payment channel

	Volume	Value
Remote	Geo 2	Geo 2
Non-remote	Geo 2	Geo 2

Table 4. Data breakdown - authentication method

	Volume	Value
SCA	Geo 2	Geo 2
Non-SCA	Geo 2	Geo 2

D – Data breakdown for all other payment transactions

D1: Data breakdown for Credit Transfers

Payment service providers should provide data both for all payment transactions as well as all fraudulent payment transactions, except for Table A5 which is applicable only to fraudulent payment transactions.

A. Transactions initiated electronically

Table A1. Total transactions and fraudulent transactions

	Volume	Value
Total Payment Transactions	Geo 3	Geo 3
Total Gross Fraudulent Payment Transactions	Geo 3	Geo 3
Total Net Fraudulent Payment Transactions	Geo 2	Geo 2

Table A2. Data breakdown - payment channel

	Volume	Value
Remote	Geo 3	Geo 3
Non-remote	Geo 3	Geo 3

Table A3. Data breakdown - authentication method

	Volume	Value
SCA	Geo 2	Geo 2
Non-SCA	Geo 2	Geo 2

Table A4. Data breakdown - reason for authentication choice

Table A4.1. Reason for authentication via SCA

	Volume	Value
Increased risk of fraud as per Art. 18 (5) RTS	Geo 1	Geo 1
Not eligible for exemption as per Art. 18 (1) RTS	Geo 1	Geo 1
Other	Geo 1	Geo 1

Table A4.2. Reason for authentication via non-SCA

Table A4.2.1 For remote payment channel

	Volume	Value
Low value	Geo 1	Geo 1
Payment to self	Geo 1	Geo 1
TRA	Geo 1	Geo 1
Trusted beneficiary	Geo 1	Geo 1

Recurring transaction	Geo 1	Geo 1

Table 4.2.1.a Transaction intervals (only with reference to TRA reason for authentication)

	Volume	Value
<100 €	Geo 1	Geo 1
≥100 and <250	Geo 1	Geo 1
≥250 and <500	Geo 1	Geo 1
≥500	Geo 1	Geo 1
	Geo 1	Geo 1

Table A4.2.2 For non-remote payment channel

	Volume	Value
Contactless low value	Geo 1	Geo 1
Unattended terminal for transport or parking fares	Geo 1	Geo 1

Table A5. Fraud types

	Volume	Value
Issuance of a payment order by the fraudster (incl. takeover)	Geo 2	Geo 2
Modification of a payment order by the fraudster	Geo 2	Geo 2
Manipulation of the payer to issue a payment order	Geo 2	Geo 2
Payer acted fraudulently	Geo 2	Geo 2

Table A6. Transactions initiated via a PISP

	Volume	Value
Transactions initiated via a PISP	Geo 3	Geo 3

B. Transactions initiated non-electronically

Table B.1. Paper based and MOTO transactions

	Volume	Value
Total Paper-based initiated transactions	Geo 2	Geo 2
Total Gross Fraudulent Paper-based initiated transactions	Geo 2	Geo 2
Total MOTO transactions	Geo 2	Geo 2
Total Gross Fraudulent MOTO transactions	Geo 2	Geo 2

D2 – Data breakdown for Direct Debits

Payment service providers should provide data both for all payment transactions as well as all fraudulent payment transactions, except for Table 3 which is applicable only to fraudulent payment transactions.

Table 1. Total transactions and fraudulent transactions

	Volume	Value
Total Payment Transactions	Geo 3	Geo 3
Total Gross Fraudulent Payment Transactions	Geo 3	Geo 3
Total Net Fraudulent Payment Transactions	Geo 1	Geo 1

Table 2. Form of consent

	Volume	Value
Consent given electronically to the PSP (e.g. EPC e-mandates model)	Geo 1	Geo 1
Consent given in other forms to the PSP	Geo 1	Geo 1

Table 3. Fraud Type (for fraudulent transactions only)

	Volume	Value
Mandate inexistence/ invalidity	Geo 1	Geo 1
Manipulation of the payer	Geo 1	Geo 1
Payer acted fraudulently	Geo 1	Geo 1

D3 - Data breakdown for Card-based Payments transactions to be reported by the payer's PSP

The payer's payment service providers should provide data both for all payment transactions as well as all fraudulent payment transactions, except for Tables A6 and A6.1 which is applicable only to fraudulent payment transactions.

A.Transactions initiated electronically

Table A1. Total transactions and fraudulent transactions

	Volume	Value
Total Payment Transactions	Geo 3	Geo 3
Total Gross Fraudulent Payment Transactions	Geo 3	Geo 3
Total Net Fraudulent Payment Transactions	Geo 2	Geo 2

Table A2. Data breakdown - card function

	Volume	Value
Payment transaction with cards with a debit function	Geo 3	Geo 3
Payment transaction with cards with a credit or delayed debit function	Geo 3	Geo 3

Table A3. Data breakdown - payment channel

	Volume	Value
Remote	Geo 3	Geo 3
Non-remote at POS	Geo 3	Geo 3

Table A4. Data breakdown - authentication method

	Volume	Value
SCA	Geo 2	Geo 2
Non-SCA	Geo 2	Geo 2

Table A5. Data breakdown - reason for authentication choice

Table A5.1. Reason for authentication via SCA

	Volume	Value
Increased risk of fraud based on trans. Monitoring outcome	Geo 1	Geo 1
Not eligible for exemption as per Art. 18 (1) PSD2	Geo 1	Geo 1
Other	Geo 1	Geo 1

Table A5.2. Reason for authentication via non-SCA

Table A5.2.1 For remote payment channel

	Volume	Value
Low value	Geo 1	Geo 1
TRA	Geo 1	Geo 1

Trusted beneficiary	Geo 1	Geo 1
Recurring transaction	Geo 1	Geo 1

Table A5.2.1.a Transaction intervals (only with reference to TRA reason for authentication)

	Volume	Value
<100 €	Geo 1	Geo 1
≥100 and <250	Geo 1	Geo 1
≥250 and <500	Geo 1	Geo 1
≥500	Geo 1	Geo 1
	Geo 1	Geo 1

Table A5.2.2 For non-remote POS payment channel

	Volume	Value
Contactless low value	Geo 1	Geo 1
Unattended terminal for transport or parking fares	Geo 1	Geo 1

Table A6. Fraud types

	Volume	Value
Issuance of a payment order by the fraudster (incl. takeover and fraudulent use of the card number)	Geo 2	Geo 2
Modification of a payment order by the fraudster	Geo 2	Geo 2
Manipulation of the payer to issue a payment order	Geo 2	Geo 2
Payer acted fraudulently	Geo 2	Geo 2

Table A6.1 Issuance of a payment order by a fraudster – fraud sub-types

	Volume	Value
Lost and stolen cards	Geo 2	Geo 2
Counterfeit cards	Geo 2	Geo 2
Card not received fraud	Geo 2	Geo 2
Other	Geo 2	Geo 2

Table A7. Transactions initiated via a PISP

	Volume	Value
Transactions initiated via a PISP	Geo 3	Geo 3

B. Transactions initiated non-electronically

Table B.1. Paper based and MOTO transactions

	Volume	Value
Total Paper-based initiated transactions	Geo 2	Geo 2

Total Gross Fraudulent Paper-based initiated transactions	Geo 2	Geo 2
Total MOTO transactions	Geo 2	Geo 2
Total Gross Fraudulent MOTO transactions	Geo 2	Geo 2

D4- Data breakdown for Card-based Payments transactions to be reported by the payee's PSP

The payee's payment service providers should provide data both for all payment transactions as well as all fraudulent payment transactions, except for Table A5 which is applicable only to fraudulent payment transactions. The geographical perspective "cross-border 1 leg outside of the EEA" relates to cards issued outside of the EEA and acquired within a Member State.

A. Transactions initiated electronically

Table A1. Total transactions and fraudulent transactions

	Volume	Value
Total Payment Transactions	Geo 3	Geo 3
Total Gross Fraudulent Payment Transactions	Geo 3	Geo 3
Total Net Fraudulent Payment Transactions	Geo 2	Geo 2

Table A2. Data breakdown - payment channel

	Volume	Value
Remote	Geo 3	Geo 3
Non-remote at POS	Geo 3	Geo 3

Table A3. Data breakdown - authentication method

	Volume	Value
SCA	Geo 2	Geo 2
Non-SCA	Geo 2	Geo 2

Table A4. Data breakdown - reason for authentication choice

Table A4.1. Reason for authentication via SCA

	Volume	Value
Increased risk of fraud based on trans. Monitoring outcome	Geo 1	Geo 1
Not eligible for exemption as per Art. 18 (1) PSD2	Geo 1	Geo 1
Other	Geo 1	Geo 1

Table A4.2. Reason for authentication via non-SCA

Table A4.2.1 For remote payment channel

	Volume	Value
TRA	Geo 1	Geo 1
Recurring transaction	Geo 1	Geo 1
Other	Geo 1	Geo 1

Table A4.2.1.a Transaction intervals (only with reference to TRA reason for authentication)

	Volume	Value
<100 €	Geo 1	Geo 1
≥100 and <250	Geo 1	Geo 1
≥250 and <500	Geo 1	Geo 1

≥500	Geo 1	Geo 1

Table A5. Fraud types

	Volume	Value
Issuance of a payment order by the fraudster (incl. takeover and fraudulent use of the card number)	Geo 2	Geo 2
Other	Geo 2	Geo 2

Table A6. Transactions initiated via a PISP

	Volume	Value
Transactions initiated via a PISP	Geo 3	Geo 3

B. Transactions initiated non-electronically

Table B.1. Paper based and MOTO transactions

	Volume	Value
Total Paper-based initiated transactions	Geo 2	Geo 2
Total Gross Fraudulent Paper-based initiated transactions	Geo 2	Geo 2
Total MOTO transactions	Geo 2	Geo 2
Total Gross Fraudulent MOTO transactions	Geo 2	Geo 2

Annex 3- Quarterly Data Reporting Data Requirements for PSPs

The first reporting takes place in 2018H2 and covers payment transactions and fraudulent payment transactions that occurred during 2018Q2.

E – Data breakdown for e-money payment transactions

Payment service providers should provide data both for all payment transactions as well as for all fraudulent payment transactions.

Table 1. Total transactions and fraudulent transactions

	Volume	Value
Total Payment Transactions	Geo 3	Geo 3
Total Gross Fraudulent Payment Transactions	Geo 3	Geo 3

Table 2. Data breakdown - payment channel

	Volume	Value
Remote	Geo 3	Geo 3
Non-remote	Geo 3	Geo 3

Table 3. Data breakdown - authentication method

	Volume	Value
SCA	Geo 2	Geo 2
Non-SCA	Geo 2	Geo 2

F – Data breakdown for money remittance payment transactions

For all tables, payment service providers should provide data both for all payment transactions as well as for all fraudulent payment transactions.

Table 1. Total transactions and fraudulent transactions

	Volume	Value
Total Payment Transactions	Geo 3	Geo 3
Total Gross Fraudulent Payment Transactions	Geo 3	Geo 3

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

For all tables, payment service providers should provide data both for all payment transactions as well as for all fraudulent payment transactions.

Table 1. Total transactions and fraudulent transactions

	Volume	Value
Total Payment Transactions	Geo 3	Geo 3
Total Gross Fraudulent Payment Transactions	Geo 3	Geo 3

Table 2. Data breakdown – payment channel

	Volume	Value
Remote	Geo 3	Geo 3
Non-remote	Geo 3	Geo 3

Table 3. Data breakdown - authentication method

	Volume	Value
SCA	Geo 2	Geo 2
Non-SCA	Geo 2	Geo 2

H - Data breakdown for all other payment transactions – H1 to H4

H1: Data breakdown for Credit Transfers

Payment service providers should provide data both for all payment transactions as well as all fraudulent payment transactions.

A. Transactions initiated electronically

Table A1. Total transactions and fraudulent transactions

	Volume	Value
Total Payment Transactions	Geo 3	Geo 3
Total Gross Fraudulent Payment Transactions	Geo 3	Geo 3

Table A2. Data breakdown - payment channel

	Volume	Value
Remote	Geo 3	Geo 3
Non-remote	Geo 3	Geo 3

Table A3. Data breakdown - authentication method

	Volume	Value
SCA	Geo 2	Geo 2
Non-SCA	Geo 2	Geo 2

Table A4. Transactions initiated via a PISP

	Volume	Value
Transactions initiated via a PISP	Geo 3	Geo 3

B. Transactions initiated non-electronically

Table B.1. Paper-based and MOTO transactions

	Volume	Value
Total Paper-based initiated transactions	Geo 2	Geo 2
Total Gross Fraudulent Paper-based initiated transactions	Geo 2	Geo 2
Total MOTO transactions	Geo 2	Geo 2
Total Gross Fraudulent MOTO transactions	Geo 2	Geo 2

H2 – Data breakdown for Direct Debit transactions

Table 1. Total transactions and fraudulent transactions

	Volume	Value
Total Payment Transactions	Geo 3	Geo 3
Total Gross Fraudulent Payment Transactions	Geo 3	Geo 3

Table 2. Form of consent

	Volume	Value
Consent given electronically to the PSP (e.g. EPC e-mandates model)	Geo 1	Geo 1
Other	Geo 1	Geo 1

H3- Data breakdown for Card-based Payments transactions to be reported by the payer's PSP

A. Transactions initiated electronically

Table A1. Total transactions and fraudulent transactions

	Volume	Value
Total Payment Transactions	Geo 3	Geo 3
Total Gross Fraudulent Payment Transactions	Geo 3	Geo 3

Table A2. Data breakdown - card function

	Volume	Value
Payment transaction with cards with a debit function	Geo 3	Geo 3
Payment transaction with cards with a credit or delayed debit function	Geo 3	Geo 3

Table A3. Data breakdown - payment channel

	Volume	Value
Remote	Geo 3	Geo 3
Non-remote at POS	Geo 3	Geo 3

Table A4. Data breakdown - authentication method

	Volume	Value
SCA	Geo 2	Geo 2
Non-SCA	Geo 2	Geo 2

Table A5. Transactions initiated via a PISP

	Volume	Value
Transactions initiated via a PISP	Geo 3	Geo 3

B. Transactions initiated non-electronically

Table B.1. MOTO card based payment transactions

	Volume	Value
Total MOTO card based payment transactions	Geo 2	Geo 2
Total Gross Fraudulent MOTO card based payment transactions	Geo 2	Geo 2
Total paper transactions	Geo 2	Geo 2
Total gross fraudulent paper transactions	Geo 2	Geo 2

H4- Data breakdown for Card-based Payments transactions to be reported by the payee's PSP

The payee's payment service providers should provide data both for all payment transactions as well as all fraudulent payment transactions. The geographical perspective "cross-border 1 leg outside of the EEA" relates to cards issued outside of the EEA and acquired within a Member State.

A. Transactions initiated electronically

Table A1. Total transactions and fraudulent transactions

	Volume	Value
Total Payment Transactions	Geo 3	Geo 3
Total Gross Fraudulent Payment Transactions	Geo 3	Geo 3

Table A2. Data breakdown - payment channel

	Volume	Value
Remote	Geo 3	Geo 3
Non-remote at POS	Geo 3	Geo 3

Table A3. Data breakdown - authentication method

	Volume	Value
SCA	Geo 2	Geo 2
Non-SCA	Geo 2	Geo 2

Table A5. Transactions initiated via a PISP

	Volume	Value
Transactions initiated via a PISP	Geo 3	

B. Transactions initiated non-electronically

Table B.1. MOTO card based payment transactions

	Volume	Value
Total MOTO card based payment transactions	Geo 2	Geo 2
Total Gross Fraudulent MOTO card based payment transactions	Geo 2	Geo 2
Total paper transactions	Geo 2	Geo 2
Total gross fraudulent paper transactions	Geo 2	Geo 2

6. Accompanying documents

6.1 Draft 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 guidelines 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, efficiency and confidence within the EEA-wide single market for payments. The Directive updates the existing rules with a view to create 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) of the Directive 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 competent authorities. Those competent authorities shall provide EBA and the ECB with such data in an aggregated form".

The growth of innovative payment services in recent years raises concerns related to the way consumer data is used; the lack of consumers' understanding of risks when inputting personal information in mobile apps without passwords; and weak authentication requirements established by merchants or payment services providers, which can result in a significant rise in fraud or alleged fraud[5].

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 payments security issues[6] and the development of the European payments services market will highly depend on the level of safety and confidence among the stakeholders involved.

The current framework about fraud data reporting is fragmented and differs across the EU. Not all Member States are collecting data on payment services in the same way. Differences include the

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

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

definition of "fraudulent payment transaction" used across countries and to the reporting methodologies applied. Moreover, the level of detail varies widely across the EU.

In conclusion, the lack of a uniform and effective fraud data reporting within the EU leaves space for an uneven level playing field across Member States and could also adversely affect consumer protection against fraud due to a weak monitoring activity.

B. Policy objectives

These guidelines aim to ensure that the reporting of fraud data by payment service providers to competent authorities is comparable and reliable within all Member States and at the EU level. This will contribute to enhancing consumer protection, promoting innovation and improving the security of electronic payment services across the EU[7] and the EEA.

Analysing and comparing fraud data between different payment providers, payment instrument and services will contribute to assessing the effectiveness of applicable regulation, identifying fraud trends and potential risks, assessing and comparing fraud data between different payment instruments and inform any future regulatory or supervisory change or action.
The recording of fraud data should also enable payment service providers 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 information were to be published, consumers could have access to reliable and updated 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

Guideline 2: General data requirements

Payment services providers could report the information required according to the following options:

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

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

[7] 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 imply higher costs compared to Option 2.1.1. The EBA however notes 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 to the other options due to the relevant amount of data to be provided and recorded.

Option 2.1.2 has been retained.

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

- Option 2.2.1: Providing only gross fraudulent payment transaction data;
- Option 2.2.2: Providing gross and net fraudulent payment data;
- Option 2.2.3: Providing gross and net fraudulent payment data, limiting the net data to only the amount of transaction that has been recovered by the reporting payment services providers (excluding other parties to the payment chain recovering part of the amount).

Option 2.2.1 would not allow competent authorities to understand and assess the responsibilities between the different payment service providers that were part of the payment chain. Option 2.2.2 would address this issue fully by requesting payment service providers to also report net fraudulent payment data. However, any given payment service provider would not be able to know the overall net figure for any given payment transaction. The payment service provider would mostly be able to provide data with regards to whether it has been able to recover some of the funds.
Only Option 2.2.3 takes this practical challenge into account, requesting providers to only report data on funds they have been able to recover. This would allow competent authorities to get specific information about the effectiveness of the security processes applied by payment services providers.

Option 2.2.3 has been retained.

Guideline 3: Frequency and reporting timelines

Payment services providers could report the data required with the following frequency:

- 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 payment services providers;
- Option 3.4: High level data are reported quarterly and detailed data are reported annually except for small payment services providers[8].

According to Article 96(6) “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

[8] 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.

competent authorities". This means that PSD2 does not preclude more frequent reporting than annual reporting, but simply provides a minimum of annual reporting.
In order to enable competent authorities to act quickly, it is reasonable to require some data more frequently than annually.
However option 3.1. is considered not feasible given that it would imply excessively high compliance costs for services providers and competent authorities.
Option 3.2 is equally considered not feasible as it would prevent competent authorities to act quickly and prevent identifying any potential issue before it grows.
Option 3.3 and Option 3.4 comply with Article 96(6) and are more proportionate that option 3.1, allowing competent authorities to record some data on a quarterly basis. Furthermore, Option 3.4 is consistent with the proportionality principle as it excludes some small payment services providers from reporting data more frequently than on an annual basis.

Option 3.4 has been retained.

Guideline 4: Geographical breakdown and reporting

Payment services providers could report the data required according to the following geographical reporting:

- Option 4.1.1: Payment service providers, including all established branches and agents, report all data to the home Member State.
- Option 4.1.2: Established branches report data separately to host Member State and payment service providers without established branches but with agents to their home Member State;
- Option 4.1.3: Established branches and agents report separately to their host Member State and payment service providers separately to home Member State.

Option 4.1.1 wouldn't provide accurate information on the number of payment transactions. Option 4.1.2 and Option 4.1.3, instead, are both able to represent better the current status of payment transactions in each Member State. Nevertheless, it is reasonable to assume that Option 4.1.3 would be excessively costly and difficult to apply for competent authorities as some money remitters have a relevant amount of agents which are also not individually registered or authorized by any competent authority.

Option 4.1.2 has been retained.

Payment services providers could report the data required according to the following geographical breakdown:

- Option 4.2.1: Payment service providers do not provide any geographical breakdown;
- Option 4.2.2: Payment service providers only distinguish between transactions within the EEA and one-leg out of the EEA;
- Option 4.2.3: Payment service providers distinguish transactions between domestic, cross border within the EEA and one-leg out of the EEA.

Option 4.2.1 doesn't provide any information about cross-border payments. This option wouldn't allow competent authorities to understand where frauds originate.

Option 4.2.2 and Option 4.2.3 provide important information about the value and the volume of cross-border payments. Despite this, Option 4.2.2 would provide only a partial figure of the issue under the scope of the guideline compared to Option 4.2.3.

Option 4.2.3 has been retained.

Guideline 5: Reporting dates

Payment services providers could report all fraudulent payment transactions according to the following reporting dates:

- Option 5.1: Fraudulent payment transaction is reported as soon as fraud is detected;
- Option 5.2: Fraudulent payment transaction is reported only when a case is closed.

Option 5.1 would allow payment services providers to report timely and fairly accurate data. In contrast, Option 5.2 could imply significant delay in reporting a case of fraudulent payments transaction.

Option 5.1 has been retained.

Guideline 6: Detailed data breakdown

Payment services providers could report the data required according to the following level of detail:

- Option 6.1: Data breakdown that differ depending on services and payment instruments used is applied;
- Option 6.2: The same data breakdown for all;
- Option 6.3: The lowest common denominator of data detail is applied.

Option 6.1 is consistent with the proportionality principle and would address potential unavailability of some payment services providers.
In contrast, Option 6.2 wouldn't be feasible due to the inability of all payment services providers to report data with the same level of detail. This option would imply also higher compliance costs.
Option 6.3 wouldn't allow competent authorities to record all fraudulent transaction cases implying weak information for a supervisory purpose.

Option 6.1 has been retained.

Guideline 7: Data aggregation

Competent authorities could aggregate the data provided by payment services providers according the following options:

- Option 7.1: Competent authorities should aggregate the data recorded in a specific and defined format under the guidelines following a specific procedure;
- Option 7.2: Competent authorities can decide with more discretion how to aggregate the data recorded.

Option 7.1 ensures a uniform and harmonised approach in the data aggregation. This option would however imply higher compliance costs for competent authorities compared to Option 7.2, although it is reasonable to state that a more integrated reporting process would facilitate the data aggregation by competent authorities making procedures more effective.
In contrast, Option 7.2 would imply differences in data aggregation processes across Member States, impeding competent authorities from providing cross-referenced data to the EBA and ECB.

Option 7.1 has been retained and the detailed way to comply will be provided outside of the guidance.

Guideline 8: Data reporting

Competent authorities could report to the EBA and ECB the data provided by payment services providers according the following options:

- Option 8.1: Competent authorities must send the aggregate data to the EBA and ECB within a specific timeline;
- Option 8.2: Competent authorities must send the aggregate data to the EBA and ECB according to a general timeline leaving more discretion to Member States.

Option 8.1 is not considered feasible due to differences in competent authorities' data reporting processes across Member States. The number of payment services providers that have to report data varies within the Member States. Furthermore, in cases where a jurisdiction has more than one competent authority, the competent authorities should co-ordinate the data recordion to ensure that only one set of data is reported for that Member State.
Option 8.2 addresses the issues mentioned above allowing competent authorities to take into account the specificities of their market when the data has to be reported to the EBA and ECB.

Option 8.2 has been retained.

D. Cost-Benefit Analysis

The aim of these guidelines is to define the set of payment transactions data to be reported to comply with the requirement under Article 96(6) PSD2. The guidelines include defining fraudulent payment transactions for the purpose of data reporting, setting out reporting methodologies and processes to be applied, in addition to the data breakdown. This is going to affect payment services providers, user of payment services and competent authorities.

The expected benefits refer to the possibility to improve the effectiveness and the quality of fraud data reporting across Member States. More harmonised reporting processes would allow competent authorities 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, its reliability and comparability will facilitate the monitoring o payment fraud, the information exchange between competent authorities, the ECB and EBA and, in turn ultimately contributing in enhancing the level of confidence in the EEA payment services markets.

Identifying and monitoring payment fraud will contribute to the better supervising and overseeing of payment fraud which in turn will contribute to the reduction of fraud, positively affecting consumers. Consumer protection against 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 would also benefit payment service providers. The use of payment services, especially innovative types of payment, across Member States will highly depend on the capacity of regulators and supervisors to reduce the risk of fraud in the market[9].

On the other hand, the implementation of these guidelines would imply compliance costs for both, competent authorises and payment services providers. These costs will mainly refer to additional reporting standards to be set out by competent authorities and to the increasing administrative burden for payment services providers.

It is reasonable to assume that most of the costs will be one-off costs in order to set up new reporting and data recording processes. In addition to this, a number of competent authorities already record fraud data, albeit with different methodologies and following different definitions. This means that the overall costs impact would be bearable and, in particular, for some Member States not be too significant. In addition, a number of payment service providers already record fraud data wither for the purpose of complying with national requirements or with industry requirements, although the data breakdown and methodology may differ, the overall costs impact are likely to be bearable and, in some cases, not be too significant.

In conclusion, the benefits expected from a better consumer protection against fraud would exceed the costs that both competent authorities and payment services provider could face. A safer payment services markets can increase the use of payment services creating new opportunities for all the stakeholders involved[10] and potentially contribute to economic growth[11].

[9] See also: European Central Bank, The future of retail payments: opportunities and challenges, Joint conference of the ECB and the Oesterreichische Nationalbank - 12-13 May 2011.

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

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

6.2 Overview of questions for consultation

Question 1: Do you consider the objectives for the guidelines as chosen by the EBA, in close cooperation with the ECB, including the link with the RTS on SCA and CSC (and in particular Articles 18 and 20 RTS), to be appropriate and complete? If not, please provide your reasoning.

Question 2: In your view, does the definition of fraudulent payment transactions (in Guideline 1) and the different data breakdown (in Annexes 2 and 3) cover all relevant statistical data on "fraud on means of payment" that should be reported? If not, please provide your reasoning with details and examples of which categories should be added to, or existing categories modified in, the Guidelines.

Question 3: Do you agree with the EBA's proposal to exempt Account Information Service Providers from reporting any data for the purpose of these Guidelines? Please provide your reasoning with detail and examples.

Question 4: Do you agree with the rationale for not including in Guideline 2.5 a requirement to report data for attempted fraud for the purpose of these Guidelines? If not, please provide your reasoning with detail and examples.

Question 5: Do you agree with the proposal for payment service providers to report both gross and net fraudulent payment transactions, with net fraudulent transactions only taking into account funds recovered by the reporting institution (rather than any other institution) as set out in Guideline 1.5? If not, please provide your reasoning with detail and examples.

Question 6: Do you consider the frequency of reporting proposed in Guideline 3, including the exemption from quarterly reporting for small payment institutions and small e-money institutions in light of the amount of data requested in Annexes 1, 2 and 3, to be achieving an appropriate balance between the competing demands of ensuring timeliness to reduce fraud and imposing a proportionate reporting burden on PSPs? If not, please provide your reasoning with detail and examples

Question 7: Do you agree that payment service providers will be able to report the data specified in Guideline 7 and each of the three Annexes? If not, what obstacles do you see and how could these obstacles be overcome?

Question 8: In your view, do the proposed Guidelines reach an acceptable compromise between the competing demands of receiving comprehensive data and reducing double counting and double reporting? If not, please provide your reasoning.

Question 9: Do you agree that prevent payment services providers should distinguish between payment transactions made by consumers and payment transactions made by other PSUs?? Please provide your reasoning with detail and examples.