From: EMA

To: Members of the EMA

Subject: Draft EBA PSD2 Guidelines on fraud reporting requirements under Art. 96(6) of PSD2

Date: 3 November 2017

Background

The second Payment Services Directive (PSD2)[1] confers on the European Banking Authority (EBA) the mandate to issue Guidelines related to the reporting of fraud data on means of payment.

On 2 August 2017, the EBA published a Consultation Paper on "*Draft Guidelines on the fraud reporting requirements under Article 96 (6) of Directive (EU) 2015/2366 (PSD2)*".

This states:

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 competent authorities. Those competent authorities shall provide EBA and the ECB with such data in an aggregated form.

The consultation closed on **3 November 2017** and the EMA sought Members' views on the proposed Guidelines to inform its response. The guidelines will apply from 13 January 2018.

The final EMA response, submitted to the EBA on 3 November is detailed below.

[1] Art 96(6)

List of Questions for Consultation

Q1: 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.

A. The EMA support the objectives for these EBA Guidelines that are identified in the Consultation Paper. Additionally, we believe that the design of the fraud reporting requirements' draft guidelines should be aligned with the *Calculation of Fraud Rates* and *Monitoring* Articles of the SCA on SCA and CSC. We would also expect that these draft Guidelines are aligned with the Guidelines on major operational or security incidents[2] and with other relevant EU Directives (e.g. 4MLD).

We are concerned that the draft Guidelines describe a one-way fraud reporting mechanism from PSPs to the relevant national competent authorities (***NCAs***).

There is no detail/guidance on a process that NCAs or the ECB/EBA may use to share aggregate fraud trend data with payment industry participants across the EEA. In the absence of such a process, EEA PSPs will find it difficult to get consistent access to insights on payment fraud trends and patterns. Therefore, we propose that the EBA defines a standardized process that NCAs will use to share aggregate payment fraud data with the regulated entities they supervise. Such detail can be introduced in the *Guidelines on fraud data reporting applicable to Competent Authorities* section of the document.

We note the statement that appears in Chapter 2 (Subject matter, scope and definitions), Clause 12 of the draft Guidelines that "*The Guidelines are subject to the principle of proportionality, which means that all PSPs 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 PSPs, depending on their size, business model and complexity of their activities*". It is not clear which entity (the EBA, the relevant NCAs) will inform PSPs of any such differences. We propose that this is clarified in the final GLs.

[2] That the EBA has developed under its PSD2 mandate [Art. 96(3)]

The EMA also wants to highlight that the original PSD2 text requires 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.*"[3] Our view is that the national competent authorities, the EBA and the ECB can fully meet their stated fraud monitoring objectives by receiving/analyzing the annual fraud data detailed in Annex 2 of these draft Guidelines. Competent authorities (i) Can also request access to the annual audit report of the methodology/model used to calculate reference fraud rates and the reported fraud rates that any PSP that uses TRA-based SCA exemptions[4] is required to make available upon request and (ii) Will receive the annual "*comprehensive assessment of the operational and security risks relating to the payment services they provide and on the adequacy of the mitigation measures implemented in response to those risks*" that PSD2 requires PSPs to provide.[5] In this context, we propose that the EBA removes the requirement that PSPs generate and submit quarterly updates to the relevant NCA as detailed in Annex 3.

Q2: 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.

A. It would be helpful if the EBA can ensure that the fraud types identified in the data breakdowns in Annexes 2 and 3 are aligned with the fraud types identified in other payment industry frameworks including the Payment Statistics Regulation (EU 1409/2013). The aim should be to avoid uncertainty and misunderstanding in the identification/labelling of fraud types for different payment instruments.

   The EMA notes the extensive reference to a *Geo 3* geographical data breakdown reference that appears in Annexes 2 & 3. According to the definition for Geo 3 (in Annex 1), this requires PSPs to report fraud transaction/volume data separately for

[3] Art 96(6) of PSD2.

[4] See Art.3 of the RTS on SCA and CSC

[5] Art 95(2) of PSD2.

all domestic, EEA cross-border, EEA cross-border with 1 leg outside the EEA; *additionally, PSPs are required to break down the reported data for each of the 31 EEA jurisdictions*. The requirement to break down reported fraud data separately for each EEA country will introduce a significant, additional workload for many PSPs that offer their services across the EEA. We believe that the stated objectives of these Guidelines would be adequately met by requesting that the PSPs report transactions that are domestic, EEA cross-border and EEA cross-border with 1 leg outside the EEA (Geo 2 definition in Annex 1); that is, without further reporting fraud data separately for each EEA territory. The relevant competent authorities can collect and process such data and share it with the ECB/EBA. The ECB/EBA can use such data to identify differences in volumes/fraud types across EEA territories with minimal additional analysis. Therefore, we propose that the Geo 3 definition is removed from Annex 1 and that all references to Geo 3 are replaced with Geo 2 in the rest of this document.

The EMA question the value of the separate "*Manipulation of the user*" fraud type introduced in Annex 2. Presumably, this fraud type aims to identify attacks carried out using social engineering or identity fraud methods. Typically, the correct identification of such methods takes some time after a fraud incident is first reported. As a result, we expect that such fraud will be in any case under-reported by PSPs. We propose that this separate fraud type is removed from the *Table of Fraud types* in Annex 2.

We also note that the *Reason for authentication via non-SCA* table in Annex 2 does not list "*Credit transfers between accounts held by the same natural or legal person*" as one of the reasons that a PSP may use to avoid completing SCA for a given transaction; this is an SCA exemption that is listed in Chapter III of the RTS on SCA and CSC. We would ask that the EBA clarify how PSPs are expected to report transactions completed using this SCA exemption.

Finally, the EMA seek further clarification on the use of the Table A6 in Data Breakdown D4 of Annex 2 and Table A5 in Data Breakdown H3 of Annex 3 (*Transactions initiated via a PSP*) to be submitted by the payee PSP. We expect that, in some business models, it will be difficult for the payee PSP (acquirer) to detect that the entity that initiates a transaction is a PISP acting on behalf of the payer rather than the payer AS-PSP. We can also envisage operational scenarios where the payee

PSP itself is acting as a PISP for a given transaction. Additionally, in most instances, fraud is first reported to the AS-PSP that manages the payment account of the party that suffers such fraud and not to the payee PSP. In this context, we would question the accuracy of the data submitted by the payee PSP using these Tables. Therefore, the EMA would propose that the requirement to report PIS-initiated transactions is removed from payee PSPs.

Q3: 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.

A. We disagree with the EBA proposal to exempt AISPs from reporting any fraud data for the purpose of these GLs. AISPs are expected to receive regular access to PSU sensitive payment data; fraudsters are expected to target AISPs with a view to unauthorised access to sensitive payment data that can then be used to mount attacks to other PSPs (e.g. through account takeover or impersonation fraud). As such, the relevant NCAs should receive some AISP fraud reporting that can be used to detect emergence (or growing impact) of fraud typologies targeting these new PSPs. We propose that the EBA introduces separate annual fraud reporting requirements for AISPs.

Q4: 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.

A. Overall, we understand the rationale behind the EBA decision to avoid including averted/attempted fraud in the fraud reporting requirements in these Guidelines.

However, it is worth noting that the use of averted fraud statistics is wide among payment industry participants and is used to assess the effectiveness of existing fraud controls. The detection of large variances in the levels of averted fraud on a country-level or among different PSP categories can be used to identify underlying weaknesses in the fraud control framework that is used by a large number of PSPs.

Q5: 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.

A. We disagree with the EBA proposal that PSPs should report both gross ***and*** net fraudulent payment transactions. The EMA view is that PSPs should ***only*** report gross fraud payment transactions since this provides a cleaner way of reporting fraud and of assessing the effectiveness of existing fraud controls. The reporting of net fraudulent transactions would only offer an indication of the effectiveness of the fraud recovery process (e.g. by using insurance policy arrangements, by leveraging their place in the payment chain etc.) used by different PSPs rather than of their fraud prevention/detection controls.

   The requirement to provide data on net fraudulent transactions will also likely introduce complex data adjustment requirements[6] for PSPs since the recovery of funds associated with a fraud incident may well take place outside the reporting period that gross fraudulent data are reported.

Q6: 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.

A. As detailed in our response to Q.1, the EMA considers that the costs of the fraud reporting requirements detailed in these draft GLs for PSPs outweigh the fraud management benefits to payment service users and to the entire payments industry.

   Specifically, the requirement to submit quarterly reporting starting from the second half of 2018 (using the templates in Annex 3) underestimates the impact on existing fraud management tools and processes of many PSPs.

[6] As detailed in Guideline 6.3

Instead, we would again propose that the requirement that PSPs submit quarterly fraud reports to the relevant NCAs is removed from these draft Guidelines and that the first annual reporting period submission takes place in 2020 to report fraudulent transactions that occurred in the first 12 months following the date of application of the RTS on SCA and CSC[7].

Q7: 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?

A. The EMA expect that many PSPs will have to invest significant resources to comply with the fraud reporting requirements detailed in these draft Guidelines. In our responses to earlier questions we have indicated our objections to:

- The quarterly reporting requirement (detailed in Annex 3),
- The start of any fraud reporting before 18 months have elapsed following the application date of the RTS on SCA and CSC,
- The requirement to report fraud transaction data for each of the 31 EEA jurisdictions.

We also seek further clarification from the EBA on:

1. The requirement that PSPs report data on all transactions and fraudulent transactions distinguishing between SCA and non-SCA transactions on a Geo 2 basis. The latter is defined to include cross-border transactions with one leg outside the EEA. However, PSD2 and the scope of application of the RTS on SCA and CSC exempt such transactions from the need to apply SCA; therefore, it is not clear why such transactions should be included in the fraud reporting requirement introduced in Table *Data breakdown – authentication method* in Annexes 2 & 3. We would propose that such reporting is carried out on a Geo 1 basis (domestic, cross-border EEA).
2. The alignment of fraud types introduced in these Guidelines with the payment fraud typologies used by existing domestic and international fraud

[7] Currently projected to be Q3/Q4 2019.

management frameworks[8] and those used by the international payment card schemes.

3. The application of fraud reporting requirements to ATM transactions involving cash withdrawals (rather than just credit transfers as referenced in Guideline 1.6b).

Q8: 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.

A. The EMA anticipate that the adoption of the fraud reporting requirements as detailed in these draft Guidelines will lead to over-reporting of fraud transactions by multiple PSPs (payer ASPSPs, PISPs acting on behalf of the payer or the payee, PSPs acting as transactions acquirers on behalf of the payee). The requirement to report both on gross and net fraudulent transactions will lead to further over reporting of fraudulent transactions

   It is not clear how over-reporting will not lead to double counting of fraudulent transactions; the Guidelines do not provide any detail on how PSP-submitted data will be reconciled and processed to produce clean datasets that identify single instances of fraudulent transactions.

   We expect that the identification of fraudulent payment transactions initiated by PISPs is likely to be particularly affected by over-reporting since both AS-PSPs and PISPs are required to identify such transactions. Our concern is that such over-reporting of fraud transactions may create the perception of inflated fraud rates that affect PISPs; we would welcome further EBA guidance to the relevant NCAs on the use of methodologies to avoid overcounting fraudulent transactions that are routinely reported by multiple industry participants.

Q9: Do you agree 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.

[8] See Financial Fraud Action UK, the EPC annual Payment Threats and Fraud Trends report etc.

A. The EMA would disagree with the proposed introduction of an additional requirement to distinguish between payment transactions involving consumers and other types of PSUs (e.g. corporate entities) in a future version of these Guidelines.

Many PSPs will find it difficult to distinguish between individual consumers and other types of PSUs (micro-merchants, small/medium enterprises, sole traders etc.) and to report transactions involving such PSUs on a consistent basis. Furthermore, we are not clear that the submission of separate transaction/fraud data would strengthen the understanding of fraud-types affecting non-consumer PSUs among NCAs, the ECB and the EBA.

Here, it is worth noting that the relevant NCAs will be able to gain insights on the impact of fraud affecting corporate PSUs by the scope of use of the TRA-based SCA exemption related "to the use of dedicated payment processes and protocols that are only made available to payers who are not consumers"[9].

[9] See Art. 18 of the RTS on SCA and CSC.