BANKING STAKEHOLDER GROUP

Replies to Questions

CONSULTATION PAPER

on Guidelines on fraud reporting under PSD2

EBA/CP/2017/13

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. Yes, alignment is with the RTS is good, but further alignment with the Guidelines on major operational or security incidents would be helpful.

   The taxonomy and terminology relating to fraud and payment instruments should be better aligned with the equivalents mentioned in the COM(2017) proposal 489 of the EU directive on combating fraud and falsifying means of payment other than cash, which repeals Council Framework Decision 2001/413/JHA. Furthermore, we note that the statistical data on payments and statistics on card fraud gathered by the ECB are carried out according to geographical breakdown criteria, which are not in line with those indicated by the EBA.

   It would be further helpful if the EBA sets out a means by which aggregate fraud data can also be shared by the EBA/ECB/NCAs with the payments industry. The EBA can for example set out a standardized process for NCAs to share aggregate payment fraud data with the regulated sector.

   We believe the impact of quarterly reporting on the regulated sector will be excessive and suggest annual reporting be implemented and that this is reviewed in 5 years. This would meet the requirements of PSD2 text without adding excessive obligations at the outset.

   Members of the BSG also suggest automated reporting to law enforcement be considered, as well as better fraud data sharing between obligated entities.

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 fraud types are aligned with the fraud types identified in other payment industry initiatives.

   There is considerable uncertainty on the impact of double reporting and the absence of provisions to address this risk. There is also concern that the Gross and Net reporting figures will give rise to uncertainty in the final figures and be unwieldy to operate in practice. We suggest a gross figure be regarded as sufficient for the time being, with a review period set out.

   Some members consider that cases of fraud where the payer has been manipulated or is the fraudster himself/herself should not fall within the base calculation of the risk coefficient as indicated in the Transaction Risk Analysis (TRA), i.e. only payments unauthorised by the payment account/instrument holder should be considered for the fraud calculation for SCA exemptions.

   It is also suggested that the tables for different product types and for different parameters be consolidated into a simpler structure.

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 suggest including AISPs in the reporting obligations to address the risk of data loss from their systems, or through their services, which can then be used to perpetrate fraud on users.

Many of the objectives cited in the Draft Guidelines relate to the aim of having an overview of fraud throughout the market, to properly observe any critical issues. To this end, all authorised market operators should be obliged to disclose their data. Excluding AISPs from the reporting obligations could fail to show a key element such as data and identity theft, which can result in fraudulent transactions. Today, the greatest threats/fraudulent methods start precisely with data/identity theft and social engineering techniques. Moreover, examining stolen data may help to establish a list of "sensitive payment data". Therefore, reporting by AISPs may provide an important contribution to recognising and understanding the scale of the phenomenon.

Other members of the BSG agree with the EBA's assumption that PSPs that only provide account information services should be excluded from the requirements of these Guidelines as they do not execute payment transactions and therefore could not report in any way "fraudulent payment transactions". So, they agree with the proposal of excluding AISPs from reporting data for the purpose of these GLs.

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. Whilst it is more difficult to identify attempted but averted fraud, some members believe that such data is helpful for industry as it can help identify trends and assist other entities that may have different strategies for fraud prevention, or may be more vulnerable to a fraud. However, an explicit and unambiguous definition of "attempted fraud" should be added. If the PSP has to report the fraud the moment it has been reported by the payer, attempted fraud by customers acting dishonestly (according to the definition of fraud in Guideline 1.1b) will always be included in the reports. Yet one can only be sure

that the fraud was indeed attempted by the payer – and in turn exclude it from the reporting – once the investigation is complete.

Some members agree with the exclusion of attempted fraud as it could make the reporting requirements incumbent on the PSPs even more burdensome and disproportionate to the potential benefit of greater precision when assessing the effectiveness of security and anti-fraud systems.

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. There is a divergence of views on this issue, with some suggesting a benefit in such a distinction and proposing an additional distinction between transferred and recovered losses. Others do not see the benefit in Net loss figures, which will be subject to much uncertainty, will be subjective, and will not inform on the risk of fraud itself which was the focus of PSD2 text.

.

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. The requirement to submit quarterly data is regarded as excessive more generally, particularly at the outset of such a provision. There will be a considerable impact on systems and this is better addressed in a more gradual

manner. Other members of the BSG suggested more frequent ad hoc reporting should be provided for.

Smaller providers should be subject to the same reporting obligations as fully authorized firms, as the risk posed is unknown and some may prove to be vulnerable.

In addition, new solutions introduced by PSD2 open the box for new solutions and business models that may give rise to new or additional risks (some of them perhaps unknown yet). It is therefore important that all entities providing these services - regardless of their size - are subject to reporting obligations. Otherwise, there is a potential risk that there will be reported minor risks that together may have significant implications for the system.

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. There is a balance to be struck between maximizing the data collected and reported and the utility derived from the data, particularly given the impact on business processes in the short to medium term. The types of transactions being identified is supported, with some members questioning the utility cost ratio for member state specific data under Geo 3. Much of this data will be yielded by home member state reporting by established institutions, and the cost of deriving member state specific data for 31 EEA member states may not be proportionate for the incremental additional information. Other members of the BSG support such data collection.

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. There is significant risk of over-reporting and double counting; we suggest considering restricting reporting in the case of four party payment systems to reporting by either the PSP of the payer or to reporting by the PSP of the payee only, as a means to minimise double counting.

   There was a view from some members that fraud reporting could be centralized for some banking and other financial institution groups and consolidated at a home member state level. Others believed member state specific data would still be required to enable those host member states to have visibility of the level of fraud in their jurisdiction.

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.

A. The proposed distinction between a consumer PSU and a business PSU is dependent on the payment product that is deployed. For some, the distinction is relatively easy, such as that for cards, but for others such as P2P platform payments, the distinction can be more difficult. The requirements to distinguish fraud data on this basis would then be more onerous and give rise to inaccurate data. Such a provision could be made subject to the type of product deployed.

   Some members are of the view that PSPs should not be required to make such a distinction for several reasons. Not only it is difficult to distinguish between consumers and corporate users in the use of some payment instrument; "non-consumers" may vary depending on the national implementations of PSD2 and

the data collected would be difficult to compare across the various PSPs. Furthermore, while for some fraud types different trends and attack mechanisms could be assess by user type (e.g. online credit transfers), the introduction of this additional distinction for all services and payment instruments identified by the EBA, in the current reporting model, would entail a heavy implementation cost that outweighs the potential benefits.

Other members support the distinction, as a means of discovering the level of corporate fraud, a phenomenon mentioned by the EBA at payments security fora.