Brussels, 31st October 2017

EACB Answer to EBA Consultation Paper on Draft Guidelines on fraud reporting requirements under Article 96 (6) of Directive (EU) 2015/2366 (PSD2)

November 2017

The **European Association of Co-operative Banks** (EACB) is the voice of the co-operative banks in Europe. It represents, promotes and defends the common interests of its 28 member institutions and of co-operative banks in general. Co-operative banks form decentralised networks which are subject to banking as well as co-operative legislation. Democracy, transparency and proximity are the three key characteristics of the co-operative banks' business model. With 4,050 locally operating banks and 58,000 outlets co-operative banks are widely represented throughout the enlarged European Union, playing a major role in the financial and economic system. They have a long tradition in serving 210 million customers, mainly consumers, retailers and communities. The co-operative banks in Europe represent 79 million members and 749,000 employees and have a total average market share of about 20%.

For further details, please visit www.eacb.coop

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Fax (+32 2) 230 06 49 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail : secretariat@eacb.coop

Introductory remarks

The European Association of Co-operative Banks has assessed the Consultation Paper on Draft Guidelines on fraud reporting under PSD2 that was released by the European Banking Authority (EBA) on 2nd August 2017. In order to ensure a consistent implementation of PSD2, we would like both to contribute to the discussion around fraud reporting and to put forward some proposals to improve the Draft Guidelines published by the EBA.

Ahead of our more detailed comments on the respective questions below, the EACB would like to highlight a general concern about the proliferation of parallel reporting systems under different pieces of upcoming EU legislation. Good examples of these new obligations can be found in the General Data Protection Regulation, the Network and Information Systems Directive, the revised Payment Services Directive including both the Guidelines on notification of major security incidents and these fraud-reporting requirements.

Overview of new reporting obligations			
Art. 33 GDPR	**Art. 96 PSD2**	**Art. 14.3 NIS Directive**	**Art. 3.1 ECB Regulation on payment statistics**
1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55.	1. In the case of a major operational or security incident, payment service providers shall, without undue delay, notify the competent authority in the home Member State of the payment service provider. 6. Payment service providers should provide at least on an annual basis, statistical data on fraud relating to different means of payments to their competent authorities.	3. Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide.	The actual reporting population shall report the statistical information to the NCB of the Member State in which the reporting agent is resident, as specified in Annex III and taking into consideration the clarifications and definitions provided in Annexes I and II

This situation is particularly alarming for smaller organisations (e.g. many co-operative banks) which resources are limited. Oversize reporting and notification requirements mean less time for dealing with the customer and for securing good safe services. Additionally, for some co-

operative banks the reporting is delegated to the central body of a co-operative group[1] which needs to verify the information/statistical data with regional cooperative banks. In this context, the EACB would like to ask the European supervisors to ensure that:

- Rules between different instances and topics are as much as possible aligned in terms of notification procedures, data formats and elements to allow re-use of available data for multiple reporting requirements;

- More generally, reporting obligations take into consideration the diversity of the banking landscape and that of co-operative groups in particular where very often the central body of the co-operative network provides the payment service function instead of or on behalf of individual PSPs. In this case, the obligation to report on fraud data should rather lay with this central body instead of the individual PSP.

Question 1: 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.

The objectives of the Guidelines as listed in pages 8 and 9 of the Consultation Paper seek to ensure that fraud data relating to different means of payments is transmitted in a reliable way to competent authorities. As a result, competent authorities will have the means to supervise that PSPs are complying with applicable rules.

The Draft Regulatory Technical Standards (RTS) on Strong Customer Authentication and Common and Secure Communication (SCA&CSC) under PSD2 aim at ensuring that personalised security credentials (PSC) are issued within a safe context and that payment service users (PSU) are not adversely affected by the exemptions to the application of SCA. Accordingly, article 18 of the Draft RTS states that an electronic payment transaction shall be considered as posing a low level of risk for the purposes of the transaction risk analysis exemption:

''where the fraud rate for that type of transaction, reported by the payment service provider and calculated in accordance with Article 19, is below the reference fraud rates specified in the table set out in the Annex for 'remote electronic card-based payments' and 'remote electronic credit transfers' respectively;''

In this framework, the EACB considers that the objectives of the Guidelines as chosen by the EBA in close co-operation with the ECB will strengthen the EBA expectation to achieve a higher degree of control, compliance and supervision of PSPs when the exemptions on strong customer authentication apply.

However, considering the link between these Guidelines and the RTS on SCA&CSC, the EACB believes that the EU institutions should urgently clarify the different timelines applicable with a particular focus on defining the framework applicable during the PSD2 transition period. In particular, we would like to request a delay of one year in the application date of the Guidelines on fraud reporting requirements (i.e. from 13 January 2018 to 13 January 2019). According to paragraph 38 of the Consultation document, ''the proposed GL apply from 13 January 2018, which means that PSPs will be required to record fraudulent transactions from that day onwards''. We

[1] Please, for further information click on the following link: http://www.eacb.coop/en/co-operative-banks-models-groups-and-networks.html

consider that an additional year is necessary to allow banks the time to adjust their IT systems to both requirements of fraud reporting in general and the link with the RTS.

In order to effectively fight against fraud, the EACB would also like to request that those PSPs reporting fraud data should also have the right to access this consolidated data. However, submitters will require assurance the data is sufficiently protected. No entity except the relevant public authorities should have access to individual data. Any publications should only be done with aggregated and anonymised data.

Additionally, the Consultation Paper sets in page 8-9 that one of the objectives that the Guidelines should achieve is to support the potential publication of fraud reports by National Competent Authorities (NCA), the European System of Central Banks (ESCB) or the European Banking Authority. The EACB would like to note that any publication of fraud data should be done avoiding both the stigmatisation of Member States with high fraud levels and the reputational damage of individual PSPs. In this context, we believe that the publication of fraud data should only take place when the appropriate measures to deal with the originating fraud incident have been effectively adopted.

Finally, the Draft Guidelines state that they ''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.'' The EACB appreciates this precision but would like to obtain further clarity about which authority will decide on the application of the proportionality principle in practice.

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.

The EACB considers that the definition of fraudulent payment transaction in Draft Guideline 1 is rather exhaustive covering most of the possible fraudulent transactions that can be carried out through different channels and means of payments. However, the EACB would like to raise the following issues:

First, according to the Draft when a fraudulent action is not executed, PSPs are not obliged to report the transaction because it is considered that the final fraud did not materialise in the end. In this context, the EACB believes that data reported under these Guidelines cannot be perceived by the authorities as reflecting the full effectiveness of the security systems put in place by PSPs as it does not consider the transactions blocked before execution.

Second, the EACB considers that the EBA should further clarify the link between the definition of fraudulent payment transactions and the fraud reference rates to be used for the exemptions on SCA. In fact, while it seems appropriate to include fraudulent transactions where the payer has been manipulated or he is the fraudster himself, on the other side they should not be considered for the risk coefficient as indicated in the Transaction Risk Analysis (TRA). It should be clear that only payments not authorized by the payer should be taken into account in relation to the calculation of fraud for exemptions to SCA.

Finally, we would like to make the following comments regarding data breakdowns in Annex 2:

- **Table A4.2.2** in page 39 for credit transfers - non-remote payment channel: these data breakdowns do not seem to be relevant for credit transfers.

- **Table A3** in page 38 for the credit transfers, **Table A4** in page 41 for card-based payments reported by the payer's PSP and **Table A3** in page 44 for card-based payments reported by the payee's PSP: we believe that the breakdowns based on the authentication method (SCA or non SCA) should be enriched. We understand that these data breakdowns do not take into account the acquisition channel of electronic payment transactions (remote payment, non-remote payment or contactless payment). Considering the obligations to reinforce security in PSD2, we believe it would be interesting to follow the authentication method used for each channel. This would be beneficial as it would make it possible to better identify the operating modes. The collection of information could be done automatically so the Payment Service Provider can reliably benchmark itself.

- **Table A5** in page 39 for credit transfers, **Table 3** in page 40 for direct debits, **Table A6** in page 42 for card-based payment transactions to be reported by the PSP of the payer, **Table A5** in page 45 for card-based transactions to be reported by the payee's PSP: we believe that data breakdowns based on fraud types should be removed from Annex 2. Indeed the EACB believes that gathering data about fraud types is very complex both from a feasibility and reliability perspective. Furthermore, the determination of the fraud type appears to be an administrative burden of analysis and information gathering for management: information obtained from customers is without guarantee of truthfulness, the only reliable information comes from the findings of police investigations and not all fraud cases are investigated by police. We believe that this data is not very relevant for Payment Service Providers because it does not inform them about the operating modes and/or authentication solutions chosen which are necessary to improve prevention.

- **Table A6.1 in** page 42 for card-based payment transactions to be reported by the payer's PSP: issuance of a payment order by a fraudster –fraud sub-types. The EACB considers that the typology used in this table is interesting and feasible with some further adjustments. Indeed, this typology focuses solely on the modalities of theft of the physical card and the use of the secret code as an authentication solution and does not cover the theft of the card data and its remote use.

- **Table A4.1** in page 38 for the credit transfers, **Table A5.1** in page 41 for card-based payments reported by the payer and **Table A4.1** in page 44 for card-based payments reported by the payee: We believe that the breakdowns based on reason for authentication deserved to be enriched. The EACB considers that the monitoring of the reason for authentication in all channels does not have a particular interest because the operating modes depend on the different channels and SCA solutions. We propose to enrich the breakdown tables with the acquisition channel.

Furthermore, the regulation of payment statistics (ECB/2013/43) requires from Payment Service Providers to report volumes and values of the different types of payment transactions being processed. All common data on payment transactions between the regulation and GL 2 and its annexes 2 and 3 should be reported only once to the competent authority.

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.

The EACB would like to make the following comments regarding the EBA's proposal to exempt Account Information Service Providers (AISP) from reporting any data for the purpose of these Guidelines.

First, we understand the rationale behind the choice to exempt AISP, but we believe that such an exemption falls outside the legal mandate of the EBA. Indeed, article 33 (2) of PSD2 states that ''The persons referred to in paragraph 1 of this Article (being natural or legal persons providing only AIS) shall be treated as payment institutions, save that tittles III and IV shall not apply to them, with the exception of Articles 41, 45 and 52 where applicable, and of articles 67, 69 and 95 to 98''. Accordingly, article 96 of PSD2 fully applies to AISP and reporting of fraud data should be envisaged also for them.

Apart from legal reasons, we consider that such an exemption will fail to capture in practice fraudulent use of online credentials where an AISP has been involved (e.g. PSC are stolen and an AISP has offered a creditworthiness assessment to grant a loan to the wrong person). This situation would reduce the effectiveness of the system and will ultimately hamper the security objectives that the EBA tries to achieve.

In addition, according to the consultation paper, we understand that the fraud reported under these Guidelines will inform competent authorities and supervisors' decisions to review security measures, to check regulatory compliance including with the RTS on SCA&CSC and to identify market-wide and PSP-specific issues relating to fraud including its source. Therefore, AISP cannot completely fall outside of this reporting system.

From a more practical perspective, we consider however that the EBA should propose a specific template for fraud reporting of AISPs that is more suitable to the nature and business activity of these market operators.

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.

The EACB agrees with the rationale for not including in Guideline 2.5 a requirement to report data for attempted fraud. Some Members of the EACB have been collecting attempted fraud data throughout for several years and are still facing important challenges regarding definitions, consistency, and the cost vs. benefit of collecting such data. It is of course important to have a "denominator" value to put fraud losses in perspective. However, the collection of genuine, non-fraud transaction values and volumes serves this purpose adequately and more objectively, what makes the collection of attempted fraud data superfluous.

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.

The EACB believes that it would be more appropriate that PSPs only report gross fraudulent payment transactions. Indeed, we consider that reporting gross fraud is more valuable than reporting net fraudulent transactions for the following main reasons:

- The approach in "gross fraud", consisting in drawing up an inventory of fraudulent operations that could not be prevented by the Payment Service Provider and led to an entry on the client's account, shows multiple benefits in terms of relevance and feasibility. It allows to consider only the real cases of fraud having impacted a payer and excludes the fraud attempts thwarted before the payment. Furthermore, it allows to collect homogeneously the amount of fraud – equivalent to the nominal values of payments – and to measure the amounts of funds misappropriated by the fraudsters. The approach in "gross fraud" facilitates the data collection of fraud and the assessment and comparison of performance in the matter of prevention and mitigation of fraud in comparison to other countries. We believe this approach answers completely to the objectives of the reporting.

- The approach in "net fraud", consisting in deducting the recovered funds and the insurances' reimbursements, allows to monitor the financial impact of fraud and the need to allocate capital. The collection of "net fraud" would vary from one Payment Service Provider to another and would not allow them to compare their performance in prevention and mitigation of fraud in country-level benchmark. Indeed, several factors of very different nature cause variations on the "net fraud" total : the extent of funds allocated to amicable or contentious recovery, the extent of reimbursements from insurances, the financial responsibility in the event of fraud as agreed with non-consumers contractually and the fraudster or beneficiary' solvability in order to obtain reimbursement. The approach in "net fraud" does not provide additional elements to reduce fraud and does not respond to the objectives of prevention measure effectiveness and risk reduction monitoring.

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

The EACB does not agree with the frequency of reporting proposed in Guideline 3. We believe that the benefits (to the objectives of the GLs) of PSPs reporting on a quarterly basis this level of detail do not outweigh the additional compliance cost (administrative burden) for PSPs to adhere to this quarterly reporting-requirement. Moreover, reporting experience has shown that fraud patterns only move slowly while any major incident would already be reported and acted upon under the major incident reporting guidelines published by the EBA.

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?

We consider the reporting requirements to be theoretically feasible. However, they are very detailed and the systems required to support such reporting are not yet in place, and therefore unforeseen issues may arise.

All the data relating to different payment channels is located in different systems and reporting needs a lot of IT-work. Some of the data have to be even collected manually. Banks need more time to adapt to these requirement – Q2/18 is too early. Transposition time is definitely needed. The EACB would like to request a delay of one year for the first quarterly reporting of high-level data under Annex 3. Indeed, instead of the first reporting taking place in 2018H2 we suggest that the first reporting of this data takes place in 2019H2 (i.e. covering transactions that occur during 2019Q2). The EACB considers that this request is consistent with our previous demand of having a delay of one year in the application date of these Guidelines and will support PSPs' efforts to put in place the new systems and mechanisms to gather the necessary data (please, see answer to question 1).

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.

The EACB would welcome further clarity on the following points:

- if the acquirer should report the fraudulent payment transactions when an economic loss is detected or only when it receives a PSU's notification;
- which report should produce a PSP that is both issuer and acquirer.

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.

No, we are currently of the opinion that such a differentiation would introduce additional complexity and require additional effort which would not produce proportional benefits. The linking of exemptions to Strong Customer Authentication with fraud prevention performance provides enough incentive for PSPs to sufficiently segment and analyse their frauds in a way that allows them to minimize losses.

Contact:

The EACB trusts that its comments will be taken into account.

For further information or questions on this paper, please contact:

- Ms Marieke van Berkel, Head of Department (m.vanberkel@eacb.coop)
- Mr Pablo Lahoz Marco, Adviser, Payment Systems (p.lahoz@eacb.coop)