Doc 0230/2019
Vers. 1.0

29/04/2019
BRU/TSI/ECSAS

European Credit Sector Associations and European Payment Institutions Federation comments on the proposal for a Council Directive amending Directive 2006/112/EC as regards introducing certain requirements for payment service providers

The European Credit Sector Associations (ECSAs) and the European Payments Institution Federation (EPIF) agree with the European Commission that fighting VAT fraud is an important objective of general public interest of the Union and of the Member States. However, it is essential that the proposed measures are actually suitable instruments for combatting VAT fraud and are proportionate in terms of the additional burden they place on banks. As will be outlined in this paper, the ECSAs and EPIF believe that the current proposals do not constitute relevant measures to fight VAT fraud and we believe the proposal will not reach its objectives as it is proposing the wrong means to the right end. **Therefore, the ECSAs and EPIF oppose the proposed directive and regulation and urge the Commission to find more effective and proportionate ways to combat VAT fraud in the field of e-commerce**. We remain at the disposal of the Commission and the Council in order to understand the suggested measures and to contribute to the common objective of tackling VAT fraud.

Together, the ECSAs represent the interests of European private, co-operative, retail and savings banks. In addition, EPIF is a representative of the non-banking payments sector. As such, together, we represent a large and significant part of European Payment Service Providers (PSPs). The approach of this letter stresses the views of banks in their capacity of PSPs as well of the view of the non-banking payments sector.

European Credit Sector Associations and EPIF concerns with the proposal

In a payment transaction, banks can take the role of either the PSP of the payer or the PSP of the payee (even both in some cases). The proposal concerns *data that allow the tax authorities to (i) identify the suppliers, (ii) verify the number of transactions and their monetary value, and (iii) verify the origin of the payments*. The bank of the payee is the only one to possess such data. However, the scope of the proposal covers all payment service providers (and hence all banks independently of whether they are the PSP of the payee or the PSP of the payer) instead.

For banks or PSPs that act on behalf of consumers only, or payer PSPs, it will be difficult or impossible to comply with the proposal, as the proposal wrongly assumes that the payer PSP has all the details on the ultimate beneficiary of the payment. This assumption is wrong for a variety of reasons.

First, various payment service providers can be involved in a transaction. Therefore, the IBAN and/or BIC as known by the payer PSP could only refer to the business account of the next payment service provider in the transaction. This next PSP is not necessary the PSP of the ultimate

beneficiary. For example, from a consumer bank point of view, a consumer account can be debited in favour of a separate card issuer – and in that case the bank can then only provide the IBAN of that card issuer (for example American Express). The consumer bank has no sight at all what happens next: the card connected to the account of the card issuer could have been used to fund a PayPal wallet, which in turn could have been used to credit a marketplace that in turn could have credited the ultimate beneficiary. From a VAT reporting point of view, this ultimate beneficiary should be targeted but the consumer bank has no sight at all on this one in this scenario (in which multiple payments could be aggregated anyhow as can be seen from the Figure 1).

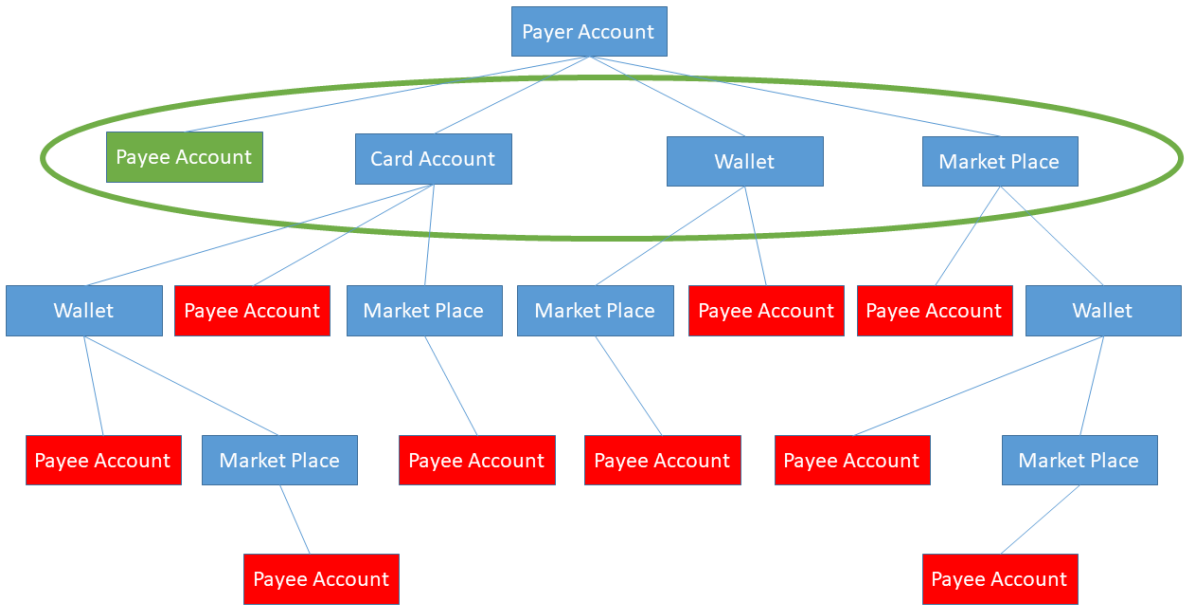

Figure 1: stacking of PSPs

In Figure 1, there is only one payee that the payer PSP can report on (subject to the conditions in the next paragraph), and that is the one in green, all the others, in red, are *hidden* behind other actors. The payer PSP can only report about the actors in the oval on top. It is only the PSP of the ultimate beneficiary (the PSP of the payee) that can provide the relevant information on the ultimate beneficiary.

Second, payer PSPs only hold data about their own customers (the payers) and they do not hold any data about the payees. The only information they have on payees is the data the payers provide to them. In addition, although an IBAN, from a payments point of view, is a unique identifier of the beneficiary, it does not disclose any information on the beneficiary, even not the country of residency of the payee – it only identifies the country where the PSP of the beneficiary is located. The same goes for the BIC, which identifies the payment service provider of the payee. This identifier also only indicates the country where the PSP resides, and does not identify the country where the payee resides. Assuming that the payer's IBAN and BIC uniquely indicate the payer's (fiscal) residence is hence simply not true.

Further, for each IBAN or account number, the PSP would have to check each quarter whether the threshold of 25 cross-border payments per payee had been reached. The volume of data generated by this obligation would be enormous and would require sophisticated software developments at a large cost. Huge volumes of unfiltered data should be examined after that by the national tax authorities in order to make a proper and deep analysis. The volumetric burden of this level of data is not proportionate to the VAT fraud – the nature of the data collection does not allow the control of the VAT application. This will require data from numerous systems for almost all payment methods, not only credit transfers and direct debits but also for payment cards, cheques and other payments methods that seem not to be in scope of the proposal, as will be outlined further in this paper. In addition, the requirement of 3-year storage of the data and the 10 days transfer rule are completely unproportioned to stop the VAT fraud. On top of this, the proposal will create an inadvertent unfair playing field, placing the burden of implementation and costs on EEA PSPs that will lead to a competitive disadvantage in favour of non-EEA PSPs, as well as to a potential migration of payers and payees to non-EEA PSPs. Furthermore, a substantial number of transactions are sent to third country payees, and therefore, there is an evident issue of regulatory asymmetry (neither payees nor PSPs in third countries/territories are obliged to cooperate with EU authorities and to respect EU law), that no obligation on PSPs in the EEA can offset. The EU should use a more targeted approach than collecting data to prevent frauds, and should use new technologies instead (for example digital ledger technologies).

The collection of the right data (that has to be recorded by the PSP of the payee, but obviously, if this PSP is outside the EEA it cannot be forced to do so) can also be an issue – typical example is the card payments where no IBAN or address of the payee are available, not to mention the additional data requested in the proposal. In the case of card payments, the payer's PSP can only rely on data that it receives via the card schemes from the payee's PSP (in contrast to credit transfers which are "*push payments*", card payments, by design, are "*pull payments*"). The payer PSPs can only keep a record of the payee's name as provided by the payee's PSP - if, for example, the names "New York Import" and "New-York Import Ltd" are mentioned, the bank has no way of knowing whether the same company is meant. Also most payment methods do not allow or cater for differentiating between payment transactions and refunds for payment transactions – in the case of a credit transfer, both the payment transaction and the refund transaction are just considered two different credit transfers. Further, there are many countries where VAT identification numbers do not exist and also, most standards used for payment methods do not currently allow for the transfer of this data element – so it will be very difficult to indicate the payee's VAT identification number.

Moreover, as per the European Central Bank[1] within the euro area, around 2.5% of credit transfers and 1.7% of direct debits initiated in 2015 were sent to an account held at a PSP resident in another country. This means that the vast majority – above 97% – were still domestic. For the European Union as a whole, the shares were 2.9% and 1.7% respectively; however, data are not available for all non-euro area countries. Compared with cross-border credit transfers and direct debits, the share of cross-border card payments is higher for both the euro area and the European Union: in the euro area, 7.6% of card payments sent from accounts held at euro area PSPs were cross-border payments; for the European Union as a whole, the share was 7.4%. Around 92.5% of EU card payments were still domestic. However, the proposal only addresses transactions where an IBAN and/or BIC are involved – this can subsequently only refer to bank transfers (direct debits and credit transfers). As the proposal aims to fight e-commerce VAT fraud, it should be noted though that current transaction identifiers for bank transfers do not require an indication whether the transaction is related to e-commerce or not. Further, Worldpay[2] estimates that in 2018 only 16% of all e-commerce transactions in the EMEA region are made via bank transfers. Worldpay also estimates that cards make 50% of these transactions; e-wallets make another 21% of these transactions. A card transaction does not involve an IBAN and or a BIC and as such, these seem not be addressed by the proposal, whilst as per the Worldpay figures cards carry the bulk of e-commerce transactions. Card transactions do have identifiers for a cardholder (PAN) and an issuing PSP (BIN) though, however, also these identifiers, like IBAN and BIC, do not identify the fiscal residency of those involved. Besides, the card industry has imposed very strong requirements on how card data is being stored and processed – these PCI-DSS[3] requirements might also impose obstacles.

Finally, data is currently stored differently by different PSPs. As a result, the contents of the information given to the register will vary according to the PSP and thus will be very difficult and costly to consolidate for the tax authorities.

[1] ECB, Economic Bulletin, Issue 3 / 2017, "Harmonised statistics on payment services in the Single Euro Payments Area", p71 (https://www.ecb.europa.eu/pub/pdf/ecbu/eb201703.en.pdf).

[2] Worldpay, "Global Payments Report. The art and science of global payments. A definitive report from Worldpay", November 2018, p15 (https://worldpay.globalpaymentsreport.com/#/home).

[3] The PCI Security Standards Council is a global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. The Council's founding members, American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc., have agreed to incorporate the PCI Data Security Standard (PCI DSS) as part of the technical requirements for each of their data security compliance programs.

Conclusion

The ECSAs and EPIF believe that the current proposals do not constitute relevant measures to fight VAT fraud and hence oppose the proposed directive and regulation and urge the Commission and the Council to find more effective and more proportionate ways such as the use of digital ledger technologies to combat VAT fraud in the field of cross-border e-commerce. Although this would still place a considerable burden on the payee PSP, potential ways to make the proposal more workable would be by explicitly clarifying that the reporting obligations would only be on the PSP of the payee, and by clarifying that the monitoring of the threshold of 25 payments should be done per IBAN. The ECSAs and EPIF remain at the disposal of the Commission and the Council in order to understand the suggested measures and to contribute to the common objective of tackling VAT fraud.