Electronic Money Association
Crescent House
5 The Crescent
Surbiton
Surrey
KT6 4BN
United Kingdom
Telephone: +44 (0) 20 8399 2066
Facsimile: +44 (0) 870 762 5063
www.e-ma.org

Richard Koch
Senior Public Policy and Public Affairs Specialist
2 Thomas More Square
London E1W 1YN
UK

4 March 2021

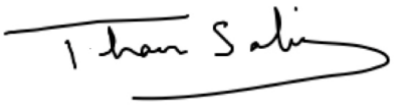
Dear Richard

Re: EMA response to OBIE CP on Evolving Open Banking Standards re: Confirmation of Payee and CRM Code

The EMA is the EU trade body representing electronic money issuers and alternative payment service providers. Our members include leading payments and e-commerce businesses worldwide that provide online payments, card-based products, electronic vouchers and mobile payment instruments. They also include a growing number of Payment Initiation Service Providers (PISPs). The EMA sits on OBIE's Implementation Entity Steering Group and participates in European initiatives under the aegis of the Euro Retail Payment Board. A list of current EMA members is provided at the end of this document.

I would be grateful for your consideration of our concerns.

Yours sincerely



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

EMA response to consultation

Q1: Do you agree with our analysis of the susceptibility of each of the 3 PISP use case categories to APP fraud? Please give reasons for your answer.

Yes, the analysis appears reasonable.

However, we note that there may be use cases within the "P2P" and "Me2Me" category where the payee details may have been validated by the PISP, and payee onboarding as robust as for the merchant initiation use case; hence, the fraud risk could - in many cases - be lower. On the other hand, there may be B2B use cases where the PISP acts on behalf of the payer and does not verify the identity of the payee e.g. integrations with accounting platforms to enable easier payment of suppliers. These use cases may be susceptible to misdirection.

The consultation paper defines P2P and Me2Me use cases as having no integration between PISP and payee domains. It is not therefore clear what the treatment would be of P2P or Me2Me use cases where there is integration between PISP and payee domains. The susceptibility of these use cases to APP fraud could be similarly low as that of the merchant-initiated use case. OBIE should consider whether the merchant-initiated use case should be expanded to include other situations where the payee details have been validated by the PISP and payee onboarding is robust. Alternatively OBIE could simply distinguish use cases where the PISP has a robust way of identifying the payee, regardless of whether it is a P2P or me2me payment.

Q2: Do you agree with our preliminary conclusions and recommendations as to the effectiveness and necessity for CoP in each of the 3 PISP use case categories? Please give reasons for your answer.

Yes/No (partially agree)

We support the conclusion that CoP serves little value in deterring APP fraud in the merchant initiated (or payee-verified) payment use case, and we therefore support Recommendation 1: that Pay.UK revise their CoP rules to accommodate the identification of MITs (or other payments where the payee has been validated to the same level as in the

MIT case) in the CoP flow. Similarly, we also support Recommendation 2 (i) and (ii): that the LSB amend the CRM Code and Practitioners' Guide to clarify that effective warnings should not be applied to merchant-initiated PISP transactions (and those where the payee details have been validated and the payee onboarded to the same standard as for MITs). However, we do not consider that the disapplication of COP or CRM warnings should be contingent on PISPs maintaining a specific (non-regulatory) standard in relation to onboarding of merchants.

We also strongly support Recommendation 3: that OBIE should update the PIS standards to accommodate messages that include information on the type of payment (i.e. MIT) to the ASPSP.

However, in relation to the remaining recommendations, whilst the rationale may be clear, applying CoP or a CRM warning in every PISP P2P or Me2Me payment flow will have a significant downstream impact that has not yet been fully explored. In our view, CoP will not be an effective remedy where the catalyst of the APP scam is a malicious payee.

We note that the CRM Code requires signatories to insert CRM warnings "where Firms identify APP scam risks in a Payment Journey". However, the OBIE Recommendation to the LSB appears to request that CRM warnings be applied to P2P PISP-initiated transactions in general. We suggest that for P2P PISP initiated transactions, the inserting of a CRM warning should be risk-based, as is already the case for other payment types under the Code provisions.

Q3i: Do you agree that there should be specific requirements relating to the onboarding and validation of payee accounts by PISPs offering Merchant Initiation via PISP?

No

Regulated PISPs, as financial institutions falling within the scope of PSD2, are subject to anti-money laundering (AML) legislation set out in the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR). This includes the conducting of customer due diligence where (i) there is a 'business relationship' with a customer or (ii) where the obligated entity 'carries out' an 'occasional transaction'

(defined as being a transfer of funds of EUR 1,000 in value or amounting to an aggregate of EUR 15,000 if combined with other related transactions).

- A 'business relationship' is defined at regulation 4 of the MLR as 'a business, professional or commercial relationship which is connected with the professional activities of an obliged entity and which is expected, at the time when the contact is established, to have an element of duration.' This is defined broadly and is likely to capture customer relationships for both PIS and AIS providers.
- 'Carrying out an occasional transaction' could conceivably include a payment initiation operation, if this amounts to the 'carrying out' of a transaction.

Customer due diligence requirements for business customers include the following:

- Identification of the customer and verification of their identity;
- Assessment of, and where appropriate, obtain information on, the purpose and intended nature of the business relationship or occasional transaction;
- Obtain and verify the name of the body corporate; its company number or other registration number, the address of its registered office, and if different, its principal place of business;
- Reasonable measures to determine and verify—
    - the law to which the body corporate is subject, and its constitution (whether set out in its articles of association or other governing documents);
    - the full names of the board of directors (or if there is no board, the members of the equivalent management body) and the senior persons responsible for the operations of the body corporate.
- Identification and verification of any beneficial owner(s);
- Where the beneficial owner is a legal person, trust, company, foundation or similar legal arrangement take reasonable measures to understand the ownership and control structure of that legal person, trust, company, foundation or similar legal arrangement.

These requirements are already robust, and must be met by all regulated PISPs in order for the PISP to maintain their licenced status. It is unclear how or whether the proposed list of merchant onboarding requirements in the consultation paper will provide any additional comfort to the ASPSP.

It is unclear how PISPs' compliance with the additional measures proposed by OBIE would be (1) monitored and (2) communicated to the ASPSP so that CoP or CRM warning would

not be applied to such transactions. There are no similar requirements for the onboarding of merchants for card-based transactions.

Q3ii: Do you agree with the proposed requirements? Are there any additional requirements that should be included? Please give reasons for your answers.

No, we don't agree that they should be imposed on PISPs.

We note that only a subset of the of the proposed requirements are necessary to provide the same level of protection/security as CoP:

- Perform an AIS consent journey to obtain the following information from their ASPSP(s) - Sort Code, account number, account name, where the entity holds the requisite permission to do so.
- Where the entity is not authorised as an AISP, undertake verification of account details in other ways, e.g. validation of copies of their bank statement during the on boarding process
- Use the 'account name' obtained as described above to populate the payee details, ensuring that there is no mechanism available to the PSU to overwrite or amend the pre-populated details either accidentally or via fraudulent manipulation of the PSU.

If a two-stage process were to be adopted, where the application of CoP to PISP payments were to take place before changes to the CRM Code, only the three requirements listed above would be relevant or necessary for the first stage.

Q4: Do you have any observations on the preliminary conclusions of this research? Are they corroborated by any proprietary research or review of the design and impact of warnings?

No comment.

Q5: Do you have views on the feasible of introducing Call to Action features in the payment process? Please give reasons for your answer.

It is not clear where in the payment flow OBIE are proposing that CTA features could be introduced. We note that section 4.4 CRM warning by the PISP in the COP-CRM Proposition

Paper does not yet address the possible 'unhappy paths' where the PSU might opt to cancel or delay the transactions following the CRM warning.

Following the detailed analysis of the research findings we would welcome further clarification and impact assessment of introducing CTAs within both the PISP and ASPSP customer journeys. For example, a CTA that includes an option to delay the payment may be possible but would depend on the PSP's permissions, as PISPs are not permitted to store sensitive data of the PSU.

Q6: Do you have views as to whether it would be constructive to include key conclusions of the research as recommendations to the LSB to add as good practice guidelines within the CRM Code & Practitioners Guidance? Please give reasons for your answer.

We agree that it would be helpful to provide recommendations to the LSB regarding the validity and effectiveness of a threshold-based application of CRM warnings.

Q7: Do you agree with our conclusion that there are 3 possible approaches to incorporating CoP requests in PIS journeys? Are there alternative options that could be considered?

Yes, subject to our responses to Q 1 and 2, where P2P and Me2Me transactions, where payee validation and onboarding is completed by the PISP, should also be exempt from the CoP requirement.

Q8: Is there commercial appetite to use each of these potential solutions to justify their development? Please give reasons for your answers.

Yes.

EMA members have, in the past, expressed commercial interest in participating in CoP. However, further work needs to be done to assist firms in understanding the likely cost and benefits before commercial appetite can be properly assessed. For example:

- More detailed analysis regarding the extent to which liability may fall on the TPP. It is accepted that designing a liability regime may be complex; however, we would welcome further exploration in this area. The existing CoP standards already have rules around liability where either sending or receiving bank makes a mistake, and also the treatment of payments where one party is not a signatory of the CRM code. It should be possible to adjust these liability rules to suit the inclusion of the PISP in messaging flow;
- We would also welcome further detail regarding the Pay.UK accreditation conditions and process;
- it would be helpful for OBIE to map out the "unhappy" customer journey, where the PSU cancels a transaction due to the CoP/CRM result in the ASPSP domain in the Proposition Paper (which will likely inform the OB Customer Experience Guidelines).

We note that OBIE envisage that Option 1 – CoP call by sending ASPSP after authentication, should always be made available. This involves the ASPSP always undertaking the CoP. If Option 1 is always available, it is unclear when, if at all, Option 2 or 3 might be supported by ASPSPs, so the question whether there is commercial appetite from PISPs for Option 2 or 3 is irrelevant.

Members also noted that, as PISP participation in COP is still some way off, Option 2 is unlikely to be feasible for some time.

Finally, some members expressed support for Option 3 as the option that would result in the best user experience, but others considered that the liability/responsibility split as well as separate interactions for Conformation of Payee and consent significantly reduces its attractiveness.

Q9: Do you agree with our conclusions that there are particular aspects of the existing CRM Code that potentially act as barriers to PISP participation? Are there others? If so, please describe.

We certainly do agree that there are a number of aspects of the existing CRM Code that act as barriers to PISP participants. The CRM Code was developed and drafted with the business models of high street banks in mind.

It is unclear whether, if the PISP were to sign up to the Code, and display the CRM warning messages themselves rather than these be displayed on the ASPSP screen, would this mean that ASPSP Code signatories are required to remove their CRM warnings for payment journeys initiated by signatory PISPs? What would be the impact on liability split between the two entities in the case of scam?

Many PISP business models do not involve the PISP coming into funds, so it is difficult to envisage how a refund would be provided by the PISP.

Q10: Do you agree that the LSB should consider modifying these barriers and would this encourage PISPs to subscribe to the Code? Please give reasons for your answers

EMA members have not expressed any appetite to sign up to the CRM Code at this stage. PISPs initiate payments, and do not execute payments, so do not come into funds. There is therefore no case for PISPs participating in a reimbursement model for funds they neither receive nor send.

The CRM Code is already subject to a number of ongoing challenges and evolutions in relation to traditional banking services; developing a PISP-appropriate extension is likely to take some time and will be challenging to fit across the variety of different business models.

Q11: Any other comments on the Consultation?

OBIE should also consider the interplay between the CRM Code, CoP, PISP payments, and:

- Roadmap item A2 b(i) Variable Repeat Payments and item A10 Sweeping
- PSR Consultation CP 21/3 on Authorised Push Payment Scams,
- PSR Consultation 21/4 on Consumer Protection in Interbank payments;

CoP and the CRM warnings may have a significant and detrimental impact on VRP and Sweeping propositions.

The PSR consultations propose changes to the UK payments systems that may have a significant impact on the necessity for CoP and the CRM warnings, which could remove the business case for PISP payments altogether.

List of EMA members as of February 2021:

AAVE LIMITED
Account Technologies
Airbnb Inc
Airwallex (UK) Limited
Allegro Group
American Express
Azimo Limited
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network Ltd
Boku Inc
CashFlows
Circle
Citadel Commerce UK Ltd
Contis
Corner Banca SA
Crosscard S.A.
Crypto.com
Curve
eBay Sarl
ECOMMPAY Limited
Em@ney Plc
emerchantpay Group Ltd
ePayments Systems Limited
Euronet Worldwide Inc
Facebook Payments International Ltd
Financial House Limited
First Rate Exchange Services
FIS
Flex-e-card
Flywire
Gemini
Globepay Limited
GoCardless Ltd
Google Payment Ltd
IDT Financial Services Limited
Imagor SA
Ixaris Systems Ltd
Modulr FS Europe Limited
MONAVATE
Moneyhub Financial Technology Ltd
MuchBetter
myPOS Europe Limited
Nvayo Limited
OFX
OKTO
One Money Mail Ltd
OpenPayd
Optal
Own.Solutions
Park Card Services Limited
Paydoo Payments UAB
Paymentsense Limited
Payoneer
PayPal Europe Ltd
Paysafe Group
Plaid
PPRO Financial Ltd
PPS
Remitly
Revolut
SafeCharge UK Limited
Securiclick Limited
Skrill Limited
Soldo Financial Services Ireland DAC
Stripe
SumUp Limited
Syspay Ltd
Token.io
Transact Payments Limited
TransferMate Global Payments
TransferWise Ltd
TrueLayer Limited
Trustly Group AB
Uber BV
Vitesse PSP Ltd
Viva Payments SA
WEX Europe UK Limited
Wirex Limited
WorldFirst
WorldRemit LTD