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

Mr Kit Shoebridge
Payments & Fintech Team, Financial Services Group
His Majesty's Treasury
1/Red
1 Horse Guards Road
London, SW1A 2HQ

By email to: Kit.Shoebridge@hmtreasury.gov.uk

22 December 2022

Dear Mr Shoebridge,

Re: Risk-based approach to payments roundtable discussion

Thank you for allowing the Electronic Money Association ("**EMA**") an opportunity to participate in the HM Treasury's roundtable policy discussions on the UK Finance's proposals for a 'risk-based approach' to payments. This letter is to set out our comments on some of the HM Treasury's questions circulated ahead of the latest roundtable meeting of 8th December 2022 which was focused on sending payment service providers.

As you will be aware, the Electronic Money Association ("***EMA***") is a UK trade association for non-bank payment service providers (such as electronic money institutions and payment institutions). A list of our members is provided at the end of this letter.

Below, we set out our general comments concerning UK Finance's proposals on risk-based approach to payments, followed by EMA response to the HM Treasury questions circulated in advance of the latest roundtable meeting.

We would be grateful for an opportunity to discuss these proposals and our comments with you at any time that suits you.

EMA General Comments

1. Efficiency of and trust in payment systems depend on immediacy and certainty of payments

The D+1 timeframe for the execution of payment orders set out in the Second Payment Services Directive (EU) 2015/2366 (as implemented in the UK by, inter alia, Regulations 86 and 89 of the Payment Services Regulations 2017 ("**PSR**")) introduced an EU-wide standard aimed at improving the efficiency of payments, and providing certainty to consumers on the length of time a payment can take. The certainty in payment execution timeframes is important for enabling financial and cashflow planning by consumers and businesses alike and reducing the time the funds are locked in transit the financial system, which is ever more so pertinent in the current economic climate (i.e. in the face of the cost of living crisis). Maintaining the D+1 standard is important in order not to undermine the trust of both the payers and payees (e.g. merchants) in the certainty provided by payment systems, the service provided by their payment service providers and competitiveness of the UK economy. A move toward less certain and slower payments would be damaging to innovation and competition in the payments sector, hindering the ability to offer new and/or improved products.

We further note that in practice, payments are expected to be completed in real time, which is the objective of Faster Payments, so that D+1 is in fact a worst case scenario in these circumstances, and would be regarded as a failure to meet service levels, disrupting many commercial transactions.

2. Slowing down of payments should only be permitted in narrowly defined circumstances

Considering the importance of <u>immediate</u> payments to commercial transactions, to efficient payment systems, and to user expectations, any exceptions to the D+1 service level legal obligations should be narrowly defined and very limited in scope.

We recognise that combatting authorised push payment ('APP') fraud whereby the customer is persuaded to make a payment to a fraudster is a complex issue. Firstly, the existing APP fraud/scam definitions are too broad (which may encompass, e.g. purchase scams, romance scams, investment scams, impersonation scams etc) - where the PSP ability to detect or prevent any particular type of scam varies. In our view, it would be more proportionate to target specific types of APP scams with suitable anti-fraud solutions. This could mean, for example, that sending PSP should only be able to delay the execution of payments beyond D+1 on suspicion of a particular type of APP scam, where the PSP ability to prevent such scam and the value of the payment justifies it.

3. The ability to delay payments must not affect SEPA payments

It is of utmost importance to ensure that UK PSPs continue to be able to participate in SEPA to send and receive payments in euros. The EMA would not support any changes which could undermine such continued participation. It is understood that this means that SEPA payments should be left out of scope of the current proposals for change.

EMA Response to HM Treasury's Questions

1. In what circumstances should the sending PSP be empowered to delay a payment (recognising the balance between supporting detecting fraud and any such provision not causing wider disruption to legitimate payments)?

a. How should the definition be framed such that it targets only the very small number of payments anticipated to require longer than D+1?

> a. Should e.g. this be defined where a payment service provider has a reasonable suspicion of fraud or is further/different provision needed?

EMA response:

Current business and user expectations are for payments to take place in real time, and D+1 provides a backstop with which PSPs comply where payments are not immediate in nature. This is an implementation of Regulation 86 of the Payment Services Regulations 2017 ("PSR 2017").

Commercial transactions require certainty of payment to be available immediately, and retail payments, particularly so. Any exception to this would therefore have an impact on both the specific transaction itself, whether it will be abandoned in favour of an alternative means of payment, or it will give rise to a complaint, but also on perception of the payment channel itself by retail users. Uncertainty will result in a preference for other means of payment that do not result in the same uncertainty.

In order to manage this risk, it is necessary to limit the scope of incidents where any delay beyond 'immediate payment' is likely to arise, and certainly any delay beyond D+1.

APP Scams relate to a very broad genre of fraud, with varying visibility to the payer PSP on the one hand, to the payer themselves and to the payee's PSP. Creating a general allowance for investigations to be carried out in order to mitigate the risk of loss to the PSP is in our view detrimental to the payment product itself, reducing fraud by reducing its overall utility for any payments.

Any allowances to disrupt the payment flow and to do so beyond the D+1 limit must be subject to a number of conditions that limit the impact of the disruption. These could include the following conditions:

1. The APP scam must be one that is capable of being observed by the PSP through monitoring, or of coming to their attention through other means such as suspicious destination accounts etc. A general allowance for all APP Scams would bring in many categories of APP fraud, many of which are largely invisible to the PSP could require extensive investigation to determine their occurrence. In other words, the more remote a fraud is from the PSP, the more time will be required to uncover its circumstances and the more delay that will ensue.

2. This is consistent with a more general condition that the scope of APP scams that PSPs would be expected to underwrite must also be those scams that are capable of being observed by the PSP. PSPs could be required to have appropriate monitoring and deterrence systems and practices, but cannot be expected to be held accountable for fraud that takes place in society as a whole and which they have little or no means of observing, detecting or preventing – even if the culmination of a successful fraud is an authorised push payment.

3. Additionally, the value of the transaction must be such as to outweigh the impact of the disruption that will be caused by delaying the payment beyond D+1.

Any proposed delay beyond D+1 must go beyond "reasonable suspicion of fraud", and must lay down conditions that must be satisfied, in order to safeguard the effectiveness of the payment system.

This is particularly relevant when considering the role that Faster Payments plays in Open Banking solutions, and the dependence of this industry on certainty of payment.

b. Should there be minimum transaction values related to being able to rely on this provision?

EMA response: We are in favour of a threshold for delaying payments beyond the backstop of D+1. There can be exceptions to avoid gaming of the thresholds by fraudsters, and these can be made subject to review by industry and regulators from time to time.

c. What requirement should be placed on the PSP to engage the customer, if they are availing themselves of the ability to pend the payment beyond D+1?

EMA response: the default position should be that the customer is immediately engaged upon any delay, but there can be exceptions where these would otherwise aid the perpetration of the scam.

> a. What actions should firms have taken prior to the lapsing of D+1, and should firms be allowed to hold payments beyond D+1 if they have not taken expected actions prior to that?

EMA response: Funds are those of payment service users, and users must have the right to dispose of their funds in whatever means they wish to do so. Once warnings are adequately given, PSP should be able to release funds to users, but simultaneously cannot be held responsible for any fraud that follows.

> b. What customer communication requirements, if any, should be placed on the sending PSP? Does Regulation 82 provide a good precedent?

EMA response: Customers should be informed by the sending PSPs if their payment is delayed beyond reasonable user expectation, and certainly beyond D+1. However, any communication requirement should not put the sending PSP at risk of assisting the fraudster. In that respect, Regulation 82 of PSR provides a good precedent.

d. Should the FCA make supplementary rules defining circumstances where a payment may be delayed? If so, what would be the scope of these circumstances?

EMA response: As per our response to question 1 above, we believe it would be more appropriate to target specific types of APP scams, where the sending PSP ability to detect or prevent such a scam (as well as the value of the payment) provides a basis for the refund obligation.

2. How long should sending PSPs be enabled to delay sending a payment beyond the existing regulatory timescales? (Should such a time-period be established in legislation or regulator rules, ideally?)

EMA response: There should be an absolute time limit following which the sending PSP could no longer delay the execution of a payment and would therefore have to execute the payment or refuse the payment. The absolute time limit can be set out in legislation. Such time limit should take into account that, the customer would not have access to their own funds during this time. Any such limit should be based on reasonableness.

3. What evidence should sending PSPs be required to record and/or report on payments they hold for longer than D+1? Should this be established in regulator rules?

a. Should stats highlighting numbers of payments beyond D+1 be published?

EMA response: No comment.

4. Are there any important considerations to make around a customer's ability to revoke payment orders, or around customer treatment (e.g. payment of interest, putting a customer into overdraft etc.)?

EMA response: No comment.

5. How should the provision be scoped from a currency perspective – e.g. should the ability to delay payments beyond D+1 apply to sterling payments (noting the potential interplay with SEPA payments)?

EMA response: The proposals to delay payments beyond D+1 for EURO transactions must be subject to agreement with the Eurosystem, and with the EPC to avoid any impact on the UK's ability to continue to participate in the SEPA framework.

6. What is the role, if any, of the payment system and its operator?

EMA response: There should be consideration of any conflicts of interest between various PSPs, different payment schemes/systems as well as the role and objectives of the governing body of Faster Payments.

7. Are there any other potential implications or considerations you would like to raise regarding sending PSPs?

EMA response: As per our general comments above, the certainty and immediacy of payments is very important for maintaining the trust in payment systems and keeping them efficient. Any measures aimed at slowing down payments thus eroding the certainty of payments must be a matter of last resort and very limited in its scope.

It is also important to ensure that the sending PSP ability to delay payments is balanced against the interests of the payer and payee in any transaction, as well as that of any third party payment service provider, such as a PIS provider. There must also not be an outcome where the current proposals provide the vehicle for de-risking certain sectors, or certain types of PSPs. Such outcomes would be extremely damaging to innovation and competition in the UK market.

We are available at any time that suits you for a discussion on the matters discussed in this letter.

Yours sincerely,

Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

Members of the EMA, as of December 2022

AAVE LIMITED
Account Technologies
Airbnb Inc
Airwallex (UK) Limited
Allegro Group
American Express
ArcaPay Ltd
Azimo Limited
Banked
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network Ltd
Boku Inc
Booking Holdings Financial Services International Limited
CashFlows
Circle
Citadel Commerce UK Ltd
Contis
Corner Banca SA
Crypto.com
Curve
eBay Sarl
ECOMMPAY Limited
Em@ney Plc
emerchantpay Group Ltd
Etsy Ireland UC
Euronet Worldwide Inc
Facebook Payments International Ltd
Financial House Limited
First Rate Exchange Services
FIS
Flex-e-card
Flywire
Gemini
Global Currency Exchange Network Limited
Globepay Limited
GoCardless Ltd
Google Payment Ltd
HUBUC
IDT Financial Services Limited
Imagor SA
Ixaris Systems Ltd
MANGOPAY
Modulr FS Europe Limited
MONAVATE
Moneyhub Financial Technology Ltd
Moorwand
MuchBetter
myPOS Payments Ltd
NOELSE PAY
NoFrixion Ltd
Nuvei Financial Services Ltd
OFX
OKTO
One Money Mail Ltd
OpenPayd
Own.Solutions
Park Card Services Limited
Paymentsense Limited
Paynt
Payoneer Europe Limited
PayPal Europe Ltd
Paysafe Group
Plaid
PPRO Financial Ltd
PPS
Ramp Swaps Ltd
Remitly
Revolut
Ripple
Securiclick Limited
Skrill Limited
Soldo Financial Services Ireland DAC
Square
Stripe
SumUp Limited
Syspay Ltd
Transact Payments Limited
TransferMate Global Payments
TrueLayer Limited
Trustly Group AB
Uber BV
Vitesse PSP Ltd
Weavr Limited
WEX Europe UK Limited
Wirex Limited
Wise
WorldFirst
WorldRemit LTD
Yapily Ltd