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

FCA by email
Financial Conduct Authority

4th October 2024

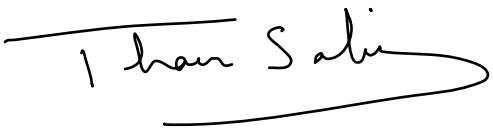
Dear FCA,

Re: EMA response to GC24/5: Authorised Push Payment Fraud: enabling a risk-based approach to payment processing

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, providing online payments, card-based products, electronic vouchers, and mobile payment instruments. Most members operate across the EU, most frequently on a cross-border basis. A list of current EMA members is provided at the end of this document.

I would be grateful for your consideration of our comments and proposals.

Yours sincerely,



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

The EMA welcomes the ability to delay a payment in order to accommodate further investigation to prevent fraud. However, we have two key areas of concern:

- **Overly bureaucratic requirements:** The current requirements do not support the time-critical and fast evolving nature of effective fraud prevention.
- **Impact on Open Banking:** It is a major concern for EMA Members that injudicious application of a delay to PISP-initiated payment could severely impact consumer usage. Therefore, we recommend that PISP payments initiated on behalf of merchants be excluded from delayed processing

EMA response to questions

Q1: Are there other factors that might increase the risk of a payment order having been made following dishonesty or fraud, which you consider we should refer to in our guidance? Are there further examples we can include in the guidance to clarify how and when payment delays legislation should be used?

The guidance [para 3.9] proposes that to meet the test of "reasonable grounds to suspect fraud or dishonesty":

> *'staff within PSPs would need to be able to demonstrate that they took reasonable steps in the particular circumstances, in the context of a risk based approach, to understand the nature and rationale of the transaction, the amount involved, the intended destination of the funds, and whether the payee appears to have any links with criminality.'*

The focus on *demonstrating* that reasonable steps were taken adds to the already substantial compliance burden on PSPs. The proposed guidance appears to require PSPs to make active inquiries into the transaction circumstances **and** gather evidence within the D+1 timeframe to meet the required standard of suspicion. Rather than focusing on the evidentiary burden, the guidance should highlight non-exhaustive examples where PSPs are likely to have met the test. The test should allow flexibility, particularly for experienced fraud analysts to use their discretion, given the fast-evolving nature of fraud.

Furthermore, we believe it is not necessary for a PSP to take steps to understand every aspect of the transaction's nature, rationale, amount and destination or the payee's links to criminality to meet the required standard of suspicion. The standard could be reasonably met based on the PSP's general knowledge of fraud patterns (which are continually evolving) and the customer's behaviour.

We do not believe it is helpful to include a list of current risk factors, as fraud evolves and what constitutes high-risk at any given time will change.

We are also concerned with linking the justification for delaying a payment to established POCA and SARs reporting standards. The threshold for suspicion required for an AML report, reached after an investigation, is far higher than the suspicion needed to justify starting an investigation.

Q2: Are there further aspects on the 'reasonable grounds to suspect threshold' that the guidance should cover? Is there anything else it would be necessary to include to ensure that industry adopts an approach that minimises the impacts on legitimate payment transactions?

The current guidance would benefit from further clarification on the types of evidence PSPs can rely on to establish "reasonable grounds to suspect" fraud. Practical examples would help PSPs apply the threshold more effectively, reducing excessive delays for legitimate transactions and ensuring fraud prevention measures are proportionate to the risks involved.

In multi-party transactions, particularly those involving PISPs or intermediary PSPs, it would be helpful to clarify the specific expectations of each party regarding fraud detection; to avoid duplication of effort and unnecessary delays.

Q3: Are there further issues about how a PSP uses the 4 business days timeframe that needs clarification in the guidance?

The EMA supports the guidance that the full four-day business period should not be used by PSPs as a general policy. Payments should be executed as soon as the PSP has established whether it should do so after contacting relevant third parties. This is crucial to minimise delays and their impact on both the payer and payees when the payment is legitimate.

Q4: Aside from PSPs having to inform customers of any delays, the reasons behind their decision and the information or actions required to help decide whether to execute the payment order, is there anything else PSPs should provide?

PSPs are required to notify the customer of the delay, its reasons, and any action needed from the payer to enable the PSP to decide whether to execute the order, as soon as possible, and within theD+1 period. This sets a high standard for notification, and we believe that providing additional information may not always be appropriate, nor feasible. As per existing standards, it is not always appropriate or possible to inform the customers of an action needed by them to resolve the payment delay, for example where there is no action the customer can take to assist the investigation. It would be helpful if the guidance clarified that PSPs need only include information about actions required from customers in cases where such actions are relevant.

Additionally, while we agree that PSPs should be required to inform customers promptly of any delays, we believe that care must be taken to avoid providing information that could inadvertently assist fraudsters. Specifically, it would be helpful to clarify that PSPs should not be required to provide detailed reasoning or descriptions of the identified risks, as this could lead to the information being passed on to fraudsters, enabling them to adjust their methods.

In certain cases, a short delay beyond the D+1 period may be reasonable for providing all necessary information to the customer, for example, where a customer's response is pending and could inform the investigation, and the action required of the customer. Clarifying the conditions under which such extensions may be permissible, particularly in cases where customer engagement is required to resolve the issue, may be helpful.

The guidance refers to the Consumer Duty guidance, suggesting that PSPs would need a *"real-time human interface, such a phone service,"* for customer communications. While call centre facilities may be suitable for some PSPs, they may not be necessary for all, especially those serving digitally savvy customers. It would be helpful to clarify that call centre access is not a mandatory requirement and that other means of communication can achieve equally, if not better, customer outcomes.

Q5: Should PSPs be obliged to notify and update PISPs about any payment delay and would there be any challenges with doing this?

We believe PISPs may be disproportionately affected by this legislation due to the increasing uncertainty regarding the timing of the payment execution when the payer's PSP delays the payment, which may undermine the success of Open Banking services. We recommend that PISP payments initiated on behalf of merchants be excluded from delayed processing.

If included, we agree strongly that a PSP must immediately notify the PISP of any payment delay, at the same time as notifying the customer, and of any subsequent changes to the payments' status. However, defining a clear and safe route for PSPs to share this information with PISPs without breaching data protection and confidentiality obligations is essential, and further guidance on this would be helpful.

Q6: Are there any further aspects of a PSP's obligations to notify relevant parties that we should clarify in the guidance?

The EMA would welcome further clarification on the notification obligations of PSPs in complex, multi-party transactions. In such cases, it would be useful for the guidance to establish a consistent notification timeframe for all relevant parties, including PISPs, payee PSPs, and other intermediaries.

Q7: Are there any further issues about notifying or communicating issues about payment delays among relevant parties that we should capture in the guidance?

The EMA supports the inclusion of further guidance on the responsibilities of PSPs, PISPs, and other relevant parties in communicating payment delays. While delays should be communicated promptly, care must be taken to avoid disclosing sensitive information that could expose the PSP to legal risks or provide fraudsters with information that could assist them. As mentioned earlier in responses to Q4 and Q5, communications should strike the right balance between transparency and safeguarding security.

Q8: Are there any issues relating to the scope of liabilities incurred by a PSP or the process of reimbursing the payer that the Approach Document should capture?

The EMA welcomes the clarification that the requirement for PSPs to reimburse customers for fees and charges incurred due to payments delay is *"narrowly constructed to apply only to interest and charges directly, and not to wider losses that a customer may experience from a payment delay, for example the loss of opportunity from an investment that the customer was unable to make in a timely way due to a payment delay being applied."* [para 3.22] While we understand that the Treasury intends to provide similar clarification in the Explanatory Memorandum to the policy, it would also be helpful to include this clarification within the Approach Document itself to ensure consistent interpretation and application by PSPs.

Furthermore, it would be helpful to clarify that this provision is intended to cover the reimbursement of the fees and charges incurred by the customer *with the delaying PSP*, rather than any other PSP involved in the payments chain (e.g. the receiving PSP). This clarification would help avoid ambiguity in terms of PSP liabilities.

Additionally, the accrual and payment of lost or incurred interest will necessitate highly complex IT system builds to reimburse what, in the case of most payment values, would be a trivial amount of interest. Payments may originate from a variety of products, each with different interest rates based on the value held in the account. Given that the reimbursement of interest is mandated by the Statutory Instrument, the establishment of a value threshold should be considered as a mitigating measure to avoid undue complexity for minimal benefit.

Q9: Is guidance needed on the cumulative effect of delays to outbound and inbound payments? Specifically, how the force majeure guidance might interact with the amendments to the PSRs 2017 execution time provisions?

Yes, further guidance is essential to address the potential cumulative effect of delays on both outbound and inbound payments, particularly in cross-border transactions or cases involving multiple PSPs. A clearer framework would help PSPs manage these situations without disrupting legitimate payments unnecessarily.

Q10: Does the guidance provide sufficient clarity on how and when the force majeure provisions can be used?

While the current guidance provides the basic principles of invoking force majeure provisions, further clarity is needed to assist PSPs in understanding the specific circumstances in which these provisions can be applied. The guidance states that the threshold for invoking force majeure is high, but more detailed examples of what constitutes "exceptional circumstances" would help PSPs determine when it is appropriate to delay payments under these provisions.

Additionally, it would be helpful to include practical guidance on the consequences of invoking force majeure, particularly in relation to fraud investigations and the potential impact on customer relations. PSPs need to understand the potential ramifications on their relationship with customers when invoking such provisions and how to communicate this effectively.

Members of the EMA, as of September 2024

Airbnb Inc

Airwallex (UK) Limited

Amazon

Ambr

American Express

ArcaPay UAB

Banked

Bitstamp

BlaBla Connect UK Ltd

Blackhawk Network EMEA Limited

Boku Inc

Booking Holdings Financial Services International Limited

BVNK

CashFlows

Circle

Coinbase

Contis

Crypto.com

Currenxie Technologies Limited

Decta Limited

eBay Sarl

ECOMMPAY Limited

Em@ney Plc

emerchantpay Group Ltd

EPG Financial Services Limited

eToro Money

Etsy Ireland UC

Euronet Worldwide Inc

Facebook Payments International Ltd

Financial House Limited

First Rate Exchange Services

Flywire

Gemini

Globepay Limited

GoCardless Ltd

Google Payment Ltd

IDT Financial Services Limited

iFAST Global Bank Limited

Imagor SA

Ixaris Systems Ltd

J. P. Morgan Mobility Payments Solutions S. A.

Lightspark Group, Inc.

Modulr Finance B.V.

MONAVATE

MONETLEY LTD

Moneyhub Financial Technology Ltd

Moorwand Ltd

MuchBetter

myPOS Payments Ltd

Navro Group Limited

Nuvei Financial Services Ltd

OFX

OKG Payment Services Ltd

OKTO

One Money Mail Ltd

OpenPayd

Own.Solutions

Papaya Global Ltd.

Park Card Services Limited

Payhawk Financial Services Limited

Paymentsense Limited

Paynt

Payoneer Europe Limited

PayPal

Paysafe Group

Paysend EU DAC

PayU

Plaid

Pleo Financial Services A/S

PPRO Financial Ltd

PPS

Push Labs Limited

Remitly

Revolut

Ripple

Securiclick Limited

Segpay

Soldo Financial Services Ireland DAC

Square

Stripe

SumUp Limited

Syspay Ltd

TransactPay

TransferGo Ltd

TransferMate Global Payments

TrueLayer Limited

Uber BV

VallettaPay

Vitesse PSP Ltd

Viva Payments SA

Weavr Limited

WEX Europe UK Limited

Wise

WorldFirst

Worldpay