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

Michael Begg
Regulatory Policy and Strategy
Payment Systems Regulator
12 Endeavour Square
London E20 1JN

By email: appscams.callforviews@psr.org.uk

15 April 2021

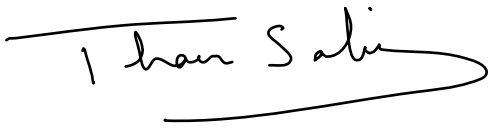
Dear Michael

Re: PSR authorised push payment (APP) scams – Call for views

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

General EMA comments

Payment service providers ("PSPs") are authorised and in the business of providing payment services; which are set out in part 1, schedule 1 of the Payment Services Regulations 2017 (UK). These services are:

(a) services enabling cash to be placed on a payment account and all of the operations required for operating a payment account;

(b) services enabling cash withdrawals from a payment account and all of the operations required for operating a payment account;

(c) the execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider—

(i) execution of direct debits, including one-off direct debits;

(ii) execution of payment transactions through a payment card or a similar device;

(iii) execution of credit transfers, including standing orders;

(d) the execution of payment transactions where the funds are covered by a credit line for a payment service user—

(i) execution of direct debits, including one-off direct debits;

(ii) execution of payment transactions through a payment card or a similar device;

(iii) execution of credit transfers, including standing orders;

(e) issuing payment instruments or acquiring payment transactions;

(f) money remittance;

(g) payment initiation services;

(h) account information services.

The role of a PSP is to provide these payment services to the payment service user. In the case of interbank payments, the PSP's role and purpose is to facilitate the transfer of funds from their customer's (payer's) account to a payee's account. This is the primary purpose of their role – it is not to provide an insurance policy with respect to every payment made by the payment service user. It would be excessive and disproportional to levy liability on PSPs for loss arising from an APP scam as APP scam loss is not causally linked (whether factually or legally) to the PSP's provision of payment services. Please note that APP-scam loss is caused by criminal acts of a third party (i.e. the scammer) and not the PSP. It is therefore not reasonable or proportional to levy liability for the criminal acts of the scammer on to the PSP.

Question 1: Do you have any comments on the data presented above? Do you have any supplementary information on customer outcomes under the CRM Code?

We have reviewed the data provided by the PSR in the Call for Evidence with interset, and would welcome further clarity in a number of areas:

1. Paragraph 3.19 provides: *One of the default requirements in the CRM Code is that when a PSP's customer has been the victim of an APP scam, they should be reimbursed by the PSP if they have acted appropriately. On the evidence we have seen, it seems unlikely that victims will have acted irresponsibly in more than 50% of APP scam cases, with the correct application of the provisions of the CRM Code (for example, giving adequate and targeted warnings) having been insufficient to prevent a scam taking place.*

   We would welcome further data analysis by the PSR regarding this conclusion, in particular the evidence referenced by the PSR that the figure of 50% of assessed losses being reimbursed is a result of PSP signatories' inappropriate application of the exception. Further explanation would better inform stakeholders considering how the issues should be addressed.

2. Paragraph 3.19 also states: *There are high numbers of cases where a victim's PSP has refused to reimburse them, and the decision has been overturned on appeal to the Financial Ombudsman.*

   We would welcome further detail regarding the 'high number' of cases overturned by the Ombudsman, as referenced by the PSR; for example, whether the suggestion is that a high proportion of the cases referred to the Ombudsman result in the overturning of the PSP's decision. Alternatively, whether this is referring to a "high number" of cases being referred to the Ombudsman in the first place.

3. We would also welcome further information regarding the reimbursement statistics set out in the graph in Figure 3; does the data also take into account reimbursement following a decision by the Ombudsman? In cases where the signatory's decision not to reimburse is overturned by the FOS and the signatory subsequently reimburses the customer, the signatory has ultimately borne liability for the loss, so this should be included in the data presented in the graph.

   We suggest that in order for stakeholders to make an informed decision with respect to outcomes of the CRM Code, the PSR should publish the overall percentage of loss assessed under the Code that are ultimately reimbursed by signatories, irrespective of whether such loss was reimbursed on the basis of a FOS decision.

Question 2: Do you have any comments on the appropriate balance of liability for APP scams costs between individuals and PSPs?

We acknowledge the increase in APP scams in the UK, exacerbated by COVID-19, and we welcome the emphasis placed on addressing this issue by regulators and government. The losses suffered by victims of this type of fraud can be significant and the impact devastating, and we support efforts by government and regulators to address the growing numbers of APP scams.

However, we do not consider it is appropriate to hold PSPs liable for loss arising from an APP scam, unless the PSP has not met their standard of care under PSD2 or other relevant legislation or guidance. Please note that under principles of English law, a PSP would not be liable to a customer for this type of loss; for that reason, we disagree with the PSR's proposed measures as set out in the consultation paper.

Placing liability on PSPs for losses incurred by victims of APPs is inappropriate for a number of reasons: (i) it is contrary to the expectations of natural justice where compensation would be expected to flow from fault (ii) it creates a disincentive for third party actors who have the ability to reduce such risk – such as the accountants or dating website providers, to act to reduce the risk; (iii) it encourages fraud by providing victims with compensation in almost all circumstances, and (iv) it leaves the underlying fraud problem, a law enforcement and government policy matter, unaddressed.

There is a clear distinction between compensation that is triggered by PSPs failing to meet a duty of care, and one that amounts to an insurance scheme for all APP Scam Fraud.

It is not in the interests of users, whether consumers or businesses, to address fraud risk through underwriting; it simply shifts the cost of the fraud back to users who will have to pay through higher fees, and fails to address the vulnerabilities in the ecosystem that give rise to the fraud in the first place.

Position supported by common law principles

The position detailed above, namely, a person is not liable when they have upheld the requisite standard of care is based on well-worn precedents of common law: at common law, where a person's actions conform to the required standard of care, they are not held liable.

In the case of payment services involving a transaction, the PSP and the payment service user (their customer) have a contract in place (the framework contract for payment services); however, the framework contract does not legislate loss sustained by the customer as a result of an APP scam.

The PSP would also not be held liable for this type of loss in tort because to the PSP has conducted themselves to the appropriate standard of care (i.e. provided the payment services with reasonable care).

We therefore consider that it would not be appropriate to attribute liability to a PSP if such liability cannot be established using fundamental English law principles.

Question 3: Do you have any comments on our analysis of what is driving the CRM Code outcomes we're seeing?

No comment.

Question 4: What could be done to ensure consistency in the outcomes of dispute resolution, and to give customers and industry transparency into how these outcomes are arrived at?

We would welcome further clarification regarding the PSR's finding that because reimbursement varies considerably across signatories (set out at paragraph 3.16), signatories must be implementing the Code incorrectly or inappropriately. Signatories may have different reimbursement rates due to a number of factors, such as different customer bases or different products, and it is unclear from the Call for Evidence whether the PSR has investigated the impact of such other factors.

We would also welcome further clarification regarding the reason for the PSR's concerns about the varying levels of reimbursement among signatories.

Question 5: Are there any other issues with the CRM Code you would like to tell us about?

There is a significant difference between levying liability on signatories of the CRM for loss arising from an APP scam and levying liability on non-signatories for the same type of loss (as proposed by measures 3A and 3B). The Code signatories have actively signed up to the Code; the basis for levying liability on Code signatories is because they have accepted such liability voluntarily. Conversely, there is no basis to levy liability on a non-Code signatory.

Other issues: The EMA response to the Lending Standards Board consultation on their Review of the CRM Code in July 2020 highlighted a number of significant provisions that make it challenging for smaller or non-bank PSPs to sign up to the Code:

1. The requirement to reimburse a customer where both firms have conformed to the Standards for Firms (with the exception of vulnerable customers);
2. The requirement to identify vulnerable customers prior to a scam taking place; and
3. The disproportionate compliance burden compared to the (current) risk posed to EMA members and their customers

The first is addressed throughout this response. We further elaborate items 2 & 3 below.

2. Vulnerable customers

In summary:

- It will be extremely difficult for all PSPs and particularly smaller PSPs to obtain enough information required to assess vulnerability in relation to a particular type of APP scam across their entire customer base;
- It is impossible to conceive of a means by which a PSP could determine from their interaction with a customer whether such vulnerability exists, other than in absolute terms, where a customer notified the PSP that they were in fact vulnerable;
- Even attempting such a feat would involve unacceptable intrusion into the lives of customers, a skill set that is closer to psychology than to payment service provision, and resources that are not available to smaller PSPs.

For these reasons, we proposed two changes to the Code with respect to vulnerable customers:

> (i) define vulnerability objectively, in broad terms (e.g. a person's age) and not subjectively with reference to the particular fraud typology. This will allow a PSP to assess whether a customer is vulnerable against certain criteria and ultimately ensure that customers who are genuinely vulnerable are assessed as such in every instance; and
>
> (ii) alter the timing of the PSP's assessment of vulnerability, namely, require the assessment to take place once the customer has reported an APP scam to the PSP.

Vulnerability is relevant to the PSP's decision whether or not to reimburse. Accordingly, whether a customer is vulnerable is only relevant at the point where the PSP is undertaking this decision (i.e. after a scam has taken place). It is unnecessary and, in some cases, not possible to obtain this information prior to a scam.

To explain further, whilst asking for information on background, financial status and financial understanding may be possible when opening a bank account, it is unlikely to be regarded as reasonable or proportionate when signing up to a single use payment product. Most e-money or payment institution accounts are specific in nature, and users are not likely to contemplate a lengthy sign-up process, or to be minded to share such information. Even if collected, there is no obvious link between fraud typologies and individual customers, except in the broadest sense; certainly not as a subjective judgement in the context of different types of frauds.

It would be more feasible and therefore allow more PSPs to participate in the Code if the process of collecting information and assessing whether a customer was vulnerable took place following reports of a scam and that this assessment was with reference to objective criteria.

3. Disproportionate compliance cost:

EMA members acknowledge the customer detriment that is being addressed by, and certainly support the aims of, the Code. However, many members have not joined because the requirements of the Code place a disproportionate compliance burden compared to the (current) risk posed to EMA members and their customers.

Whilst EMA members support the use of tools such as Confirmation of Payee, transaction monitoring, freezing of queried funds and ongoing customer education, there are many additional requirements the Code imposes that are not proportionate to their APP-scam volume, which is a fraction of that experienced by the existing signatories of the Code.

These include:

- Transaction monitoring: whilst EMA members do have transaction monitoring systems, the Code provisions aren't suited to the business model of PSPs offering occasional or single-use products. i.e. controls to identify potential APP Scams based upon transaction data are only effective if the PSP is able to view sufficient transaction history to produce a result;
- Ongoing compliance costs: exposure to a regular audit, ongoing reviews, data submissions;
- APP-scam specific training for staff and agents, when exposure to APP-related fraud is low; and
- The requirement to provide 24/7 reporting of scams when firms are not set up with such capability.

This is understandable, as the Code was designed to mitigate a risk to which banks - where customers tend to hold their main deposit accounts – are much more exposed. The EMA would therefore strongly resist the mandating of the Code for non banks for the primary reason that the cost of compliance is hugely disproportionate to the APP scam risk observed in this sector.

Mandating the adoption of the Code for all PSPs in the UK, regardless of risk or exposure to APP scams, or of business model, would create a barrier to entry for smaller or new PSPs wishing to enter the market. Instead a risk-based approach should be adopted that takes into account firms' business models and exposure to APP fraud in order to ensure consumers are appropriately protected.

Question 6: Do you have any comments on this measure, or its effectiveness and proportionality? For example, do you have feedback on the information we propose for publication outlined above, or on who should publish the data?

The EMA supports further transparency measures where they can benefit payment service users or the industry; however, some of the reporting measures proposed could result in duplication of effort and data, and may therefore be of limited use (in addition to what is already available) to payment service users.

The EMA does not support measures that are designed to "name and shame" PSPs into accepting liability for an APP scam (a liability they would otherwise not incur under law). "Shaming" is an ineffective tool to compel compliance, and will likely not reduce the

incidence of APP fraud. Any data collected from PSPs in furtherance of this measure should be published in aggregate form. In addition, publishing data organised by individual firms may affect payment service users' rights with respect to their personal data. Accordingly, any data published as a result of this measure must be in aggregate form.

PSPs are required to provide detailed payment fraud data to the FCA on a 6-monthly basis, pursuant to their regulatory obligation to file fraud reports (REP017). REP017 contains a similar data item to APP fraud: "manipulation of the payer" fraud, for which PSPs are required to report both volume and value of fraudulent transactions, by payment type, as well as whether strong customer authentication was applied to the payment and any relevant exemptions.

The PSR could consider incorporating the APP scam data categories the PSR wish to elicit from PSPs into the existing REP017. Combining APP scam data categories into REP017 (where such categories are not already included in REP017) would reduce duplication of work for both the reporting PSP and the respondent (i.e. the FCA).

It therefore follows that we consider the FCA to be the appropriate entity to collate APP scam data (in the context of collating data reported using REP017).

Question 7: Do you have any comments on this measure, or its effectiveness and proportionality? For example, do you have feedback on its feasibility, how it could work, or whether the issues and requirements set out would be best dealt with by a working group?

We do not consider standardised shared fraud scoring is an effective nor proportional measure.

First, this measure would not be effective because it would likely not be possible to create standardised fraud scores that sufficiently represent the risk of every type of transaction, in a way that can be recognised and accepted by all PSPs. Each PSP takes into consideration many differentiating factors, such as different products and customer bases with differing transaction profiles when developing their fraud scoring system. It would be extremely challenging to develop a 'one-size-fits all' fraud scoring system for the industry.

As the PSR notes, PSPs already have existing fraud risk systems and controls that have been specifically tailored to their own products and customers. It would not be proportional from a cost perspective, to replace these systems with a new system that may not be any more effective in terms of reducing APP scams for their business model.

We further note that this proposed measure would give rise to a number of risks. For example, a standardised system's effectiveness would be significantly (and quickly) reduced simply by a fraudster learning the generic scoring system and creating measures to avoid high risk ratings. This would be advantageous to a fraudster because

they could apply this knowledge when transacting with all PSPs. The effect of these measures must be explored in detail before any proposals to implement them.

An alternative approach might be to develop functionality at the payment scheme level to communicate more data between sending and recipient PSPs, for example data regarding the purpose of payment (where known), or the status of the intended recipient (business or customer). This would give the recipient PSP more data on which to base a judgement regarding the relative APP scam risk associated with that payment, and assist them in being able to identify trends or payment accounts with certain types of activity indicative of APP scammer accounts.

Question 8: Do you have any comments on Measure 3A? For example, do you have feedback on the design, or its effectiveness and proportionality?

Please see our response to question 9 below.

Question 9: Do you have any comments on Measure 3B? For example, do you have feedback on the design, or its effectiveness and proportionality?

Effectiveness:

We agree with the PSR's assertion that PSPs' underwriting of customers' APP scam losses will create a 'moral hazard' and increase the likelihood of first-party fraud; this would defeat the PSR's overall objective of reducing APP scams by creating a favourable environment for payment service users to engage in a different type of fraud (i.e. fraud perpetrated by the payer rather than the payee).

Measures 3A and 3B will not give effect to the PSR's overall objective of reducing APP scams. We consider implementing 3A and/or 3B will result in more victims being reimbursed for their loss; however, it will not reduce APP scams overall. If the PSR wishes to increase consumer protection measures in this area (as opposed to reducing APP scams), a more effective route would be to introduce a legislative requirement to provide a certain clearly defined level of consumer protection, and then allow PSPs to develop their own solutions to meet those obligations.

Proportionality:

We consider that measures 3A and 3B would likely result in an increase in the cost of using the Faster Payments scheme, which will be borne by PSPs and could ultimately be passed to consumers. If the Scheme rules placed the payer's PSP under an obligation to reimburse the APP scam victim and then recover funds from the payee PSP, FPS would have to develop operational procedures to manage that process, and any subsequent inter-PSP disputes. This would increase operational costs, which would

have to be covered by PSPs and would inevitably increase the cost of each FP transaction.

The impact of any increase in cost is felt much more by PSPs that offer payments as service (i.e. non-bank PSPs), as they do not benefit from the cross-subsidisation afforded by banks. Whilst they may be able to put in place technical and operational measures that reduce the risk that their customers might suffer from APP scams, it is much harder for them to absorb the cost of an APP scam, or the cost increase of FPS scheme fees. It is therefore crucial that a sensible balance is struck between protection for customers where the PSP has failed in their duty of care, and where an individual has authorised a payment, with all possible information provided and support offered by the PSP.

One factor that may improve proportionality of any proposal could be to exclude purchase scams from scope. Purchase scams pose specific challenges to PSPs: transactions that are the subject of a purchase scam are difficult to detect using traditional fraud control methods, as many indicate normal spending levels and patterns. It is often difficult for firms to detect whether the scam is in fact a civil dispute instead. UK law already provides recourse for consumers in this context. We note that although volumes of purchase scams are high, the values tend to be lower, and thus overall impact on consumers more limited.

Other issues to consider:

Future of UK payments: The PSR should consider these proposed measures in the wider context of the UK payments strategy, including a future migration to a New Payments Architecture (NPA), which is designed to provide a skeleton underlying infrastructure over which overlay services can compete to provide better services to consumers and businesses alike. With the move to innovative use of instant payments and, by extension, reduced transactions carried out using the card schemes, it is essential that Faster Payments offers an economically viable option in comparison to those other schemes. A higher cost associated with using Faster Payments will make the case to use Faster Payments over other payment systems less compelling. In fact, increased fraud liability, coupled with increased operating cost, may make some innovative PSP business models completely unviable, and will increase the complexity of a future migration of FPS to the NPA.

Equivalence with the EU: The EMA further notes that imposing a new level of liability on PSPs that is too onerous may affect UK PSPs' ability (i) to trade with the EU; and (ii) to remain competitive with international PSPs. UK PSPs' access to SEPA is dependent on a level of regulatory equivalence with the EU; further reducing this equivalence by imposing additional liability mechanisms may significantly affect UK PSPs' (and by extension, their customers') access to payment services in the EU.

Exceptions: Please note that for measures 3A or 3B to be feasible, the exceptions to reimbursement would have to be expanded. Currently, the only available exceptions to

reimbursement is first-party fraud, and where the loss does not arise from an APP scam. These must be expanded, for example, to include situations where the customer is asked by the PSP to provide information relating to the payment and the customer omits certain information. Alternatively, it must be a requirement for the customer to be completely transparent and assist the PSP with respect to the payment in order to successfully claim reimbursement.

Question 10: Do you have any comments on these issues? For example, do you have feedback on whether we should use a direction or a rule change to pursue these measures, or whether Bacs should be included?

If the PSR wishes to increase consumer protection measures in this area (as opposed to reducing APP scams), a more effective route would likely be to propose the tabling of a legislative requirement that sets out a certain clearly defined level of consumer protection, and then allow PSPs to develop their own solutions to meet those obligations. This would give consumers certainty regarding the level of consumer protection they can expect in relation to all payments, regardless of the payment mechanism used, and PSPs greater ability to manage the risk, and therefore the cost to the business of the additional liability.

Question 11: Do you have any comments on our proposal to conduct an equality impact assessment for any measures developed following this call for views?

No comment.

Members of the EMA, as of April 2021

AAVE LIMITED
Account Technologies
Airbnb Inc
Airwallex (UK) Limited
Allegro Group
American Express
Azimo Limited
Bitpanda Payments GmbH
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
HUBUC
IDT Financial Services Limited
Imagor SA
Ixaris Systems Ltd
Modulr FS Europe Limited
MONAVATE
Moneyhub Financial Technology Ltd
MuchBetter
myPOS Europe Limited
OFX
OKTO
One Money Mail Ltd
OpenPayd
Optal
Own.Solutions
Oxygen
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
Snowy Pay Ltd.
Soldo Financial Services Ireland DAC
Square
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