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

APP Scams Team
Payment Systems Regulator
12 Endeavour Square
London E20 1JN

Email to: appscamsdata@psr.org.uk

15 September2023

Re: PSR CP23/6 on Maximum Liability and CP 23-7 on Gross Negligence

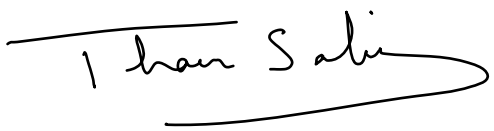
Dear APP Scams team,

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 large number of smaller Payment Service Providers. A list of current EMA members is provided at the end of this document.

We welcome the opportunity to respond to the PSR's CPs on Maximum Liability and Gross Negligence, as they will impact a large number of PSPs, including several EMA members.

I would be grateful for your consideration of our concerns.

Yours sincerely



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

Summary

The EMA has followed and engaged in industry developments with respect to APP scams from the outset in September 2016 when Which? submitted their super-complaint to the PSR.
We have:

- participated in the PSR's APP Scams Contingent Reimbursement Model Steering Group and contributing to the development of the CRM Code;
- responded to the LSB Call for Input on the CRM Code (June 2021)
- responded to the LSB CRM Code Consultation (October 2020)
- responded to the Pay.UK Consultation on an FPS Levy (October 2019)
- responded to the PSR's CP 17/2 on PSR-led work to mitigate the impact of scams, including a consultation on a contingent reimbursement model
- responded to the PSR's CP 21/3 Authorised push payment scams – call for views
- held a conference call with PSR representatives to discuss the PSR's proposals as set out in CP 21/3 Authorised push payment scams – call for views
- responded to the PSR's CP 21/10 Authorised push payment (APP) scams
- held a conference call with PSR representatives and EMA members to discuss the PSR's proposals as set out in CP22/4 Authorised push payment scams: requiring reimbursement
- responded to CP 22/4 Authorised push payment scams: requiring reimbursement
- responded to CP 23/4: APP fraud reimbursement requirement – draft legal instruments
- responded to CP/6 APP fraud: Excess and maximum reimbursement level for FPS and CHAPS
- responded to CP 23/7 APP fraud: The consumer standard of caution

In all of these interactions, we have put forward principled arguments and reasoning in relation to levying liability on PSPs for loss arising from APP scams and related issues.

To date, the PSR has not been able to refute our arguments nor have they substantively addressed our concerns.

To reiterate:

- We, PSPs, are not insurers of last resort.
- There is no basis for requiring PSPs to reimburse customers for all types of APP fraud. The PSR's reimbursement policies are inconsistent with principles of English law and go beyond the legislative intent of section 72 of the Financial Services and Markets Act 2023.
- The PSR has provided no evidence that their reimbursement policies will not increase fraud in the UK. In the PSR's stakeholder session on reimbursement held Friday 7 July 2023, **the PSR expressly stated they had not carried out any testing with respect to these policies prior to implementation and do not have any primary data to rely on as to indicate that their reimbursement policy will function as intended.** The PSR acknowledged that any data that industry could provide would be helpful and that they otherwise rely on data from UK Finance. As a competition regulator, we would expect the PSR to, at least, obtain some data and test their policies to see if they will function as intended before imposing them on the industry.

CP 23-6 on the excess and max liability

Questions

Question 1: Do you agree that PSPs should be free to apply a partial excess, as well as not levy an excess at all, should they want to?

Yes, we agree PSPs should be free to apply an excess.

We do not agree that the excess cannot be applied to vulnerable customers. PSPs will still have to deploy resources and incur costs in order to process the reimbursement claim and this will add to the operational demand on PSPs (which the PSR says is a factor in setting the excess); this is irrespective of whether the customer is vulnerable or not.

In addition, although we understand vulnerable customers may be more likely to fall victim to a scam, we do not agree that the risk of moral hazard is lower in this category of customer and have seen no data to suggest this is the case. We expect that vulnerable customers should also be required to exercise an appropriate degree of caution and so the excess should be applied to them equally.

Question 2: Are these factors the correct ones when considering the excess?

The PSR also seems to be considering (para 3.15) whether the level of excess means PSPs will not attempt to prevent fraud of the type that typically causes loss around the level of excess. We do not consider this a relevant factor – it is clear that the PSR expects firms to prevent and investigate all types of fraud and any concerns like this can be monitored through PSP data and reporting.

Question 3: Is there anything else we should consider when setting the level for the excess?

Question 4: We are seeking views on whether the excess should be a fixed amount or a percentage of the fraud value. Should the excess be a fixed value, a percentage or a percentage with a cap? If fixed, what value should it be and why? If a percentage, what amount and why? If a percentage with a cap, what amount and what should the cap be?

Our first preference is to apply a percentage excess; however, this is permitting that the percentage is meaningful. If it is not meaningful we do not view it as worth the operational demand to apply the excess and explain it to consumers. The example provided in paragraph 3.17:

> *If the percentage excess was 10%, a customer who was defrauded out of £30,000 would receive 90% of their claim back. The customer would, therefore, receive £27,000 as a reimbursement.* [3.17; CP 23-6]

is a meaningful amount. It would be sufficient as to deter the customer pursuant to their 'moral hazard' and it would be sufficient to cover the PSP's operational costs in terms of operating as the insurer of last resort.

Our answer to this question is therefore that we support a percentage excess permitting this is meaningful.

The "percentage with a cap" option, as described in the CP, has strong potential to not be meaningful. For example, the example given in paragraph 3.22:

> *Or, if the excess was 10% with a cap of £250, a customer defrauded out of £100 would receive 90% back, which would be £90. If they were defrauded out of £10,000, they would receive £9,750. [3.22; CP23-6]*

Capping an excess at GBP 250 whilst the PSP pays out an insurance policy of GBP 9,750 is not meaningful and increases the operational demand on PSPs without real benefit as compared to a fixed excess.

In saying that, if the PSR is to impose a policy that results in an excess that is not meaningful, we would support the option that is easiest to implement at an operational level. Accordingly, if the PSR's policy

is to impose an excess that is trivial, which we consider to be anything less than 5% of the total amount, we support a fixed excess of the highest amount possible.

The PSR has given PSPs only until 2 April 2024 to implement their reimbursement policies; having a fixed excess is a straightforward concept that firms can operationalise and calibrate their systems within the very short (and unreasonable) timeframe imposed by the PSR.

Question 5: Do you have any data, evidence or views to suggest how an excess should be calibrated?

Please see our response to Q4.

Question 6: Should the excess remain static? Increase with inflation? Some other metrics? Not increase at all?

The excess should remain static, and should be recalibrated in the event that evidence transpires that the PSR's policy decision with respect to the excess is inappropriate or otherwise inadequate for any reason.

Maximum reimbursement

Question 7: Do you agree that the maximum reimbursement level should be applied to all consumers, including those who might be classed as vulnerable?

There would appear to be a question missing here. The PSR has not consulted on the amount of the reimbursement, which the PSR are proposing to be set at £415,000. The PSR is only consulting on how the maximum reimbursement level should be applied. Is it therefore the PSR's intention to impose a rule without consulting on it first?

We consider that the maximum level of reimbursement proposed is far too high. We invite the PSR to compare the maximum reimbursement levels with the capital requirements for PSPs who are not banks i.e. electronic money institutions ("**EMIs**") and payment institutions ("**PIs**").

The Electronic Money Regulations 2011 provide that initial capital requirements for EMIs are EUR 350,000. The Payment Services Regulations 2017 provide that capital requirements for PIs are up to EUR 125,000.

The PSR is proposing that EMIs and PIs take on more liability than the amount of capital they are required to hold, at law. **It is unclear how such a proposal can be considered proportionate and reasonable.**

Even just one claim in excess of the initial capital level could push a PSP into insolvency and/or breach of its capital requirements.

We do not expect PSPs to be able to insure against this type of unquantifiable risk, or if insurance is eventually made available, we anticipate it will be cost prohibitive.

There is therefore significant risk that a maximum liability of this level will push PSPs several out of business, reducing competition and innovation for consumers. Even applying a limit on the value of faster payment transactions will not assist, given that APP scams may occur over several transactions which are aggregated together.

Question 8: Are these factors the correct ones when considering the maximum reimbursement level?

The PSR should consider applying different caps to different size PSPs. There are significant differences between capital requirements and resources across the industry, and it is arbitrary to apply the same cap for all, when all other similar regulatory fees etc. are calculated on the basis of revenues and volumes. Applying the same cap to all PSPs means will result in firms being subject to entirely different prudential risks across the industry. The threat of prudential breach and/or insolvency is not required to incentivise smaller PSPs.

In addition it is not clear how the PSR has applied the existing factors in setting an arbitrary level to mirror the FOS cap:

- **Level of PSP liability:** as set out at the response to Q7, the high amount of PSP liability has been disregarded and no consideration given to the number of PSPs this will push into regulatory breach and/or insolvency
- **Ability to cover majority of cases:** the proposed cap on maximum reimbursement covers nearly 100% of APP scams – this is not a mere majority, this is nearly all fraud cases. A majority of fraud cases would be covered by the much lower cap of £30,000, see further detail at responses to questions 9 and 10 below.
- **Incentivise fraud prevention:** There is no data to suggest that a lower cap of £30,000 would not cover all fraud types and incentivise PSP anti-fraud measures to the same extent.

Paragraph 2.5 of the Consultation Paper states:

> *In June and July 2023, we held engagement sessions with industry trade bodies, PSPs, and consumers groups on what values would be appropriate. The aim of these sessions was to gather initial views from our stakeholders to inform the questions and options we are presenting in this consultation.*

The EMA attended these sessions. In the PSR Stakeholder Session held Friday 7 July 2023, industry representatives argued strongly against the GBP 415,000 liability cap. In paragraph 2.5, the PSR state they have engaged with industry on what values would be appropriate. Our records from these events indicate little to no industry support that this level of liability is appropriate. All stakeholders at the sessions attended by the EMA have disagreed with the PSR's proposed policy; yet the evidence and views provided by stakeholders at that session appear not to have been taken into account, and proceeded anyway.

Question 9: Are there any other factors we should consider?

The data provided in the CP states that 99.72% of APP fraud volume is reimbursed up to and including GBP 85,000 [paragraph 4.12].

The same table further provides that 99.98% of APP fraud volume is reimbursed up to and including GBP 410,000 [paragraph 4.12].

The difference between these percentages is 0.26.

This means that for the sake of this small margin, the PSR is willing to run the risk of sinking a small PSP.

We invite the PSR to substantiate how a cap of GBP 415,000 is proportionate and reasonable. See also our response to Q10 below.

Question 10: Do you gather any data that would show what type of cases are likely to fall outside the maximum reimbursement level?

In the absence of collating independent data, we invite the PSR to review UK Finance's data on APP fraud again, and not to draw conclusions from the truncated data set out in the CP.

UK Finance aggregate data from 2022 indicates that 96.67% of fraud are cases below GBP 10,000. This means that the PSR could set the maximum reimbursement level at GBP 10,000 (or even a slightly higher number such as GBP 30,000 as to align with the Consumer Credit Act 1974 section 75 rights) and cover 99.72% of APP scams. However, it appears that for the sake of ensuring 99% of APP scams are reimbursed (rather than 96%), the PSR is willing to run the risk of sinking a small PSP.

We urge the PSR to set a reasonable liability limit; the current policy of GBP 415,000 is not proportionate, and based on UK Finance data an overwhelming majority of scams (i.e. a factor the PSR says is relevant in setting the cap) will be reimbursed if the maximum limit is GBP 30,000. There does not appear to be any rationale to substantiate levying such a significant liability for the sake of outlying cases, especially given the potential impact on smaller PSPs.

We support setting a liability limit of GBP 30,000. This level ensures that a significant majority of APP fraud cases (99.72%) are reimbursed, whilst protecting small PSPs from outlying cases of hundreds of thousands of pounds that would sink them.

Applying the £30,000 limit also reflects existing legislation offering protections to consumers that have suffered loss caused by a third party other than the financial institution required to make a payout. This limit has been introduced by statute and applied in a more equivalent scenario.

Question 11: Should the maximum reimbursement level align with the Financial Ombudsman Service going forward? Increase by inflation? Some other metrics? Not increase at all?
There is no reason to mirror the liability cap applied to the FOS.

The amount the FOS can award is as high as GBP 415,000 because the FOS provides redress where a PSP has actually breached their obligations or has not treated the customer fairly. What is under consideration here is a liability limit for an insurance policy, and not liability flowing from fault. These are completely different standards and therefore incomparable.

The PSR is making PSPs the insurer of last resort. The role of the FOS is not to adjudicate insurance policies; it is to provide an avenue for redress for the customer.

Using the FOS limit in this case is unsubstantiated. There is a basis for using the Section 75 rights limit from the Consumer Credit Act 1975 – on which there can be broad agreement.

Question 12: What factors should we consider as part of the review of a maximum reimbursement level?
The PSR should, in the first instance, revise the initial maximum reimbursement level as it is disproportionate and unreasonable before considering any review.

Relevant factors should be to align with a relevant basis for the cap, i.e. if this is based on s.75 of the CCA, it should be reviewed at the same time as the CCA.

Bank of England questions re CHAPS
Question 13: Do you agree that the current ombudsman service limit of £415,000 should be the maximum reimbursement level for APP fraud claims in CHAPS?

We do not support the policy of making PSPs the insurers of last resort for APP scams for transactions over Faster Payments or for CHAPS.

However, in saying that, EMA members do not participate in CHAPS so we will not comment further on these questions.

Question 14: For CHAPS, should the maximum reimbursement level be applied to all consumers?

Question 15: For CHAPS, do you gather any data that would show how many and what type of cases are likely to fall outside the maximum reimbursement level?

Question 16: Should the maximum reimbursement levels for Faster Payments and CHAPS diverge now or in the future?

Question 17: For CHAPS, should the maximum reimbursement level align with the ombudsman service going forward? Increase by inflation? Some other metrics? Not increase at all?

Question 18: Should a limit higher than £415,000 be adopted instead for CHAPS, and if so, what level?

CP 23-7 on gross negligence

Question 1: Do you agree that the PSR should specify the standard of care that PSPs can reasonably expect of consumers? Please provide reasons for your answer.

Yes, the PSR should specify the standard of care consumers are required to discharge in order to be reimbursed.

This is a standard requirement for an insurance policy so we consider it would also be the case here.

Question 2: Do you agree that the standards of care specified by the PSR should be exhaustive, and that PSPs should not be able to introduce additional standards through their contractual relations with consumers? Please provide reasons for your answer.

We agree the standard of care required should be uniform and therefore specified by the PSR; however, in saying that, the current standard of care proposed by the PSR is not adequate or reasonable. So, if the current proposed standard of care were to be adopted, PSPs would need to introduce additional standards by contract in order for reimbursement to function properly.

For example, the PSR provide:

> 2.20 ***We envisage two scenarios in which a consumer might understandably not comply, or fully comply, with an information request by a PSP****. The first is where the PSP either seeks information that, judged objectively, is not necessary to evaluate the claim, or where the information sought is disproportionate to the value or complexity of the claim. Consumers should not be expected to comply with such requests.*
>
> 2.21 *The second is where a PSP makes an information request which is proportionate, but where there are emotional, psychological or other complexities which result in the customer providing no, or inadequate, disclosure in response. In such a scenario, the customer may have complicated, circumstantial reasons for not wishing to make some disclosures to their PSP. We do not consider that reluctance or unwillingness by a customer to respond to information*

requests would, in and of itself, necessarily constitute valid grounds for refusing a reimbursement claim. Nor would it automatically equate to gross negligence.

2.22 ***PSPs should consider that, where a consumer is unable or unwilling to respond, or adequately respond, to an information request by their provider, this may be indicative of vulnerability****. Providers should take care to ensure that they do not mistakenly categorise vulnerability as gross negligence in such circumstances.*

Part of the standard cannot feasibly be permitting reimbursement in cases where the customer is unable or unwilling to provide information. In a case where the customer is unable or unwilling to provide information to the PSP, whatever the reason, the PSP would not even be able to meet its reporting obligations towards Pay.UK in respect of that particular scam. The PSP would have minimal information to report and not be able to comply with its own obligations in this instance.

So, we agree that the standard of care should be specified by the PSR but it must be reasonable and feasible, in the circumstances. The current proposed standard of care as set out in the CP would require PSPs to introduce additional standards simply to comply with their own obligations.

Question 3: Do you agree that the burden of proof should fall on the PSP to demonstrate that a consumer – through gross negligence – has failed to meet one or more of the standards at paragraph 3.2? Please provide reasons for your answer.

Please see our response to Q4 below.

Question 4: Do you agree that PSPs should not be able to introduce, through their contractual relations with consumers, terms or conditions that shift the burden of proof onto consumers, or seek to reduce the burden on providers? Please provide reasons for your answer.

Please see answer to question 1. In summary, our answer is yes permitting the standard of care proposed by the PSR is reasonable and otherwise feasible, in the circumstances. The standard of care currently proposed is not reasonable or otherwise feasible in the circumstances as it does not allow PSPs to meet their own obligations, for example, reporting obligations.

We invite the PSR to consider commercially available insurance policies when determining the standard of conduct required from policy-holders. The reimbursement proposals of the PSR make PSPs the insurers for loss sustained from APP scams, so this response will draw upon a standard UK, commercially available insurance policy in order to demonstrate a policy-holder standard of conduct generally accepted by industry. It will refer to Bupa's 'Bupa By You: Policy Benefits and Terms'.

Question 5: Do you agree that consumers should be expected to have regard to tailored, specific warnings raised by their PSP before a proposed authorised push payment has been executed, where those warnings make clear that the intended recipient of the payment is likely to be a fraudster? Please provide reasons for your answer.

Yes. PSPs should be able to deny reimbursement to a customer who proceeds to send a payment to a fraudster after receiving a warning. The professed reason for mandatory reimbursement is to incentivise PSPs to reduce scams – the incentive is surely weakened if customers don't need to pay heed to warnings, even those that are specific and tailored to them and the scam.
However, please note the following points:

- In order for the PSP to give warnings that are effective in the circumstances, there **must be a further requirement levied on the customer that they are truthful when interacting with the PSP at all times**.

In the PSR's stakeholder session on reimbursement held Friday 7 July 2023, industry representatives present on that call unanimously agreed that in order for reimbursement to operate effectively, the customer must be truthful when interacting with the PSP. However this has not been reflected in policy subsequently proposed by the PSR. A requirement to be truthful allows the PSP to help a customer avoid a scam; if the customer is untruthful or otherwise attempts to obfuscate the situation by withholding information, it is not possible for the PSP to do everything within its ability to prevent the customer from being scammed.

To demonstrate by way of accepted industry practice, Section 1.4 of the Bupa By You: Policy Benefits and Terms' provides:

We do not have to pay a claim *if you or a Dependant break any of the terms and conditions of membership, which are related to the claim.* ***If there is reasonable evidence that you or a Dependant did not take reasonable care in answering our questions (by this we mean giving false information or keeping necessary information from us) then*** *if this was:*

- *intentional, we may treat your or (if applicable) your Dependant's cover* ***as if it never existed and refuse to pay all claims***
- ***careless****, then depending on what we would have done if you or they had answered our questions correctly, we may treat your or (if applicable) your Dependant's cover as if it never existed and refuse to pay all claims (in which case you may need to repay any claims we have paid and we will return any subscriptions you have paid in respect of your or (if applicable) your Dependant's cover), change your or their cover, or we could reduce any claim payment.*

We consider that the PSR should include a requirement such as this in the PSR's final policy statement on this matter. It is accepted practice within the insurance industry so there is no reason why it cannot be applied to this insurance policy.

- Paragraph 2.9 of the guidance in Annex 2 provides: *The warnings should be consumer, scam, and transaction specific.* It is clear that the PSR's intention is for the PSP to offer a personalised service to the customer in that the warning must be "consumer specific". The PSR is going beyond the scope of the obligation imposed on them by Section 72 of the Financial Services and Markets Act 2023 to impose a reimbursement requirement through Faster payments; there is no obligation on the PSR to require PSPs to offer a personalised service to individual customers – not even the Consumer Duty does that: *We do not expect firms to tailor all communications to meet the individual needs of each customer or to ensure that each customer understands all of their communications.* [Paragraph 8.37; FG22-5 Finalised non-Handbook Guidance for Firms on the Consumer Duty].

- As discussed, the warnings must be "*consumer, scam, and transaction specific".* Please note that the PSP does not have sufficient information in order to provide a warning this detailed. We have reiterated this point numerous times in various interactions with the PSR / consultation responses since 2016. The scammer does not communicate with the customer over the PSP's platform. The PSP offers a payment account; it does not offer functionality for the customer to communicate with the fraudster. The communications take place over social media. The PSP is only involved at the very end of the fraud when the customer makes the payment to the fraudster. The PSP does not see any communications between the customer and the fraudster; it does not have access to their messaging over social media. The PSP does not have access to enough information in order to provide a warning to the specific standard as envisaged by the PSR. A warning of this nature would only be feasible if there was a competing requirement (as we have stated above) for the customer to be truthful with the PSP at all times. Therefore, if the customer was interacting with the PSP prior to the scam, the PSP could ask the customer questions about the transaction, analyse the facts, determine the typology and provide a

warning that was tailored to the customer's circumstances and be effective. Without some way in which to access further information (either seeing the customer's communications with the fraudster that takes place over another platform or asking the customer to provide truthful information) there is no feasible way that a PSP can provide a warning this specific. We note that this level of interaction also causes a significant amount of friction to the customer journey, which will frustrate the majority of customers that are not victims of scams.

- Separately, there should be clarity over receiving PSPs' obligations to reimburse when a sending PSP has failed to issue appropriate warnings – it is not acceptable that a receiving PSP with no ability to meet this requirement should be required to pay out 50% of a claim which would have been refused had the sending PSP complied with its obligations.

Question 6: Do you have any other comments on the requirement to have regard to warnings, taking into account the draft policy document at Annex 1 and the draft guidance at Annex 2?

Paragraph 2.8 of the guidance in Annex 2 provides:

> PSPs can expect their customers to have regard to tailored, specific warnings raised by the provider before an authorised push payment is executed, where those warnings make clear that the intended recipient of the payment is likely to be a fraudster. *Only in circumstances where the PSP can demonstrate that the customer has, as a result of gross negligence, not had regard to such warnings can a reimbursement claim be refused.*

This paragraph introduces a further (lower) standard of conduct, which reduces the usefulness of providing warnings. The customer does not fail to have regard to the warnings because they acting with gross negligence. The customer failing to have regard to the warnings cannot be separated into two categories of acting with or without gross negligence. The customer's not having regard to warnings should automatically be classified as gross negligence.

Further, paragraph 2.10 provides:

> *Although consumers should have regard to adequately constructed warnings, a consumer proceeding with a transaction despite these warnings should not automatically be deemed to have been grossly negligent. The degree of negligence that may be deemed to rest with the consumer should consider, in addition to any other relevant factors:*
> *• the specificity and nature of the warnings provided by their sending PSP*
> *• the complexity of the scam to which the consumer has become victim*
> ***• any claims history from the consumer suggesting a propensity to fall for similar types of scams***
> *• whether the PSP can reasonably be expected to have paused or otherwise prevented an APP from being executed*

We suggest that this paragraph 2.10 should be deleted from the guidance as it imposes a further (lower) standard of conduct which reduces the efficacy of providing warnings. The standard as advertised by the PSR is "the requirement to have regard to warnings"; accordingly, the standard required should be "to have regard to warnings".

The standard to be considered should not include "*any claims history from the consumer suggesting a propensity to fall for similar types of scams".* Any prior claim for reimbursement for an APP scam should disqualify or, at least, significantly curtail a customer's ability to claim again. This would be the case with an insurance policy whereby a policy-holder's premium would increase or they would be denied subsequent reimbursement following a claim to reflect the level of risk they posed to the insurance provider.

The same principles should apply here as PSPs are acting as the insurer for APP scams.

Further, please review FOS case reference number DRN-3910502. In this case, the FOS reduced the complainant's award by 50% because the complainant had been scammed in similar circumstances only 6 months prior. The FOS decided that the complainant should have been more aware of scams having been scammed previously.

So, in practice, an earlier claim usually has the effect of increasing a policy-holder's premium and/or reducing a complainant's award. It does not have the effect of making a policy-holder / claimant MORE eligible for reimbursement – it curtails their eligibility to claim. Why would it be any different here? PSPs are not absolute guarantors. Consumers must take some responsibility.

Question 7: Do you agree that consumers should be subject to a standard to promptly notify their PSP when they suspect they have, or may have, fallen victim to an APP scam? Please provide reasons for your answer.

Yes. However, this appears to be redundant because a policy-holder will always need to notify their insurer in the event they wish to claim and it is likely they will want their policy paid out "promptly" in any case. It is in the customer's own personal interests to do this.

In saying that, there should be a cut-off point at which the customer may no longer claim. We note the PSR has proposed 13 months. This time frame is adequate and reflective of the PSRs 2017, however, 13 months alone is an inadequate and oversimplified standard because the customer may claim for any long-term scam as long as the last payment took place in the last 13 months, and/or scams that occurred prior to the introduction of the PSR's reimbursement requirement. This means that a customer may claim for a fraud that has been perpetuated over several years (including years prior to the PSR's reimbursement requirement, the CRM Code, Which?'s super complaint). This would not be the case with an insurance policy. Eligibility to claim does not cover a period of time prior to the policy's being in place. The same industry-accepted concept should therefore apply here; eligibility to claim only attaches at the point at which the PSR's direction is in force, and the relevant fraud must occur during the 13-month period following this point in time. The requirement to reimburse customers for long-term scams that occur over a period of longer than 13 months should only apply to transactions within the 13-month period, not before.

Question 8: Do you have any other comments on the prompt notification requirement, taking into account the draft policy document at Annex 1 and the draft guidance at Annex 2?

Paragraph 2.15 of Annex 2 appears hardly worth mentioning:

> *When assessing whether a consumer has notified them promptly, PSPs should not rely upon any delay in notification from a consumer that has been caused by the provider's own reporting systems.*

When there is so little guidance provided, it does not seem necessary to include such a redundant statement.

Question 9: Do you agree that consumers should be subject to a standard to respond to reasonable and proportionate information requests from their PSP, where those requests are necessary to establish whether the consumer is the victim of an APP scam, or where they are necessary under our 'stop the clock' policy? Please provide reasons for your answer.

Yes. Customers should be required to respond to requests for information truthfully and promptly. The PSR have not included a requirement for customers to respond truthfully (please see response to

question 5 outlining that this is essential) and have otherwise been apologetic about the customer's ability to respond to such information requests:

> *The second is where a PSP makes an information request which is proportionate, but* ***where there are emotional, psychological or other complexities which result in the customer providing no, or inadequate, disclosure in response****. In such a scenario, the customer may have complicated, circumstantial reasons for not wishing to make some disclosures to their PSP.* ***We do not consider that reluctance or unwillingness by a customer to respond to information requests would, in and of itself, necessarily constitute valid grounds for refusing a reimbursement claim****. Nor would it automatically equate to gross negligence.* [paragraph 2.21 of Annex 2]

This is not in line with industry standard. For example, Section 2.6.1 of the Bupa By You: Policy Benefits and Terms' provides:

> *When we need to ask your doctor for more information in writing, about your consultation, tests or treatment for insurance purposes, we'll need your permission. The Access to Medical Reports Act 1988 or the Access to Personal Files and Medical Reports (NI) Order 1991 give you certain rights which are:*
>
> - *You can give permission for your doctor to send us a medical report without asking to see it before they do.*
> - *You can give permission for your doctor to send us a medical report and ask to see it before they do.*
>
> *– You'll have 21 days from the date we ask your doctor for your medical report to contact them and arrange to see it.*
>
> *– If you don't contact your doctor within 21 days, we'll ask them to send the report straight to us.*
>
> *– You can ask your doctor to change the report if you think it's inaccurate or misleading; if they refuse, you can insist on adding your own comments to the report before they send it to us. – Once you've seen the report, you can withdraw your permission for it to be sent to us.*
> - **You can withhold your permission for your doctor to send us a medical report. If you do, we'll be unable to see whether the consultation, test or treatment is covered by your policy, so won't be able to give you a pre-authorisation number or confirm whether we can contribute to the costs.**

Here, under a standard UK insurance policy, if the policy-holder refuses to furnish the insurance provider with the relevant information, the insurance provider "will not be able to contribute to costs" i.e. will not reimburse the customer.

Why would the case be different for APP scams? As previously explained, the example above is from a health insurance policy so the policy-holder would be required to furnish information relating to their health which is arguably more sensitive that any information that would be requested by the PSP in the context of an APP scams claim.

There should be no allowance for the customer not to respond to a reasonable and proportionate information request from the PSP. This must be an absolute condition of reimbursement. Responding to reasonable and proportionate information requests from an insurance company is industry standard if that policy-holder wishes to be paid. Accordingly, the same standard should apply here.

EMA members report instances when customers submit complaints alleging they have been defrauded, and providing only by the payment details, i.e. date and value of payment, and sort code and account

number of the payee. Under the PSR's proposals PSPs would be required to reimburse in these instances, despite having insufficient information to investigate. Please note that most PSPs would also have no visibility over whether a customer refuses to disclose more information because of emotional, psychological or other complexities or because they were not actually victim of a fraud.

In addition, there should be a requirement on sending PSPs to investigate rather than accept claims without sufficient information, including a requirement to use information provided by the receiving PSP in their investigations. It is not acceptable that a receiving PSP should be required to pay out 50% of a claim which would have been refused had the sending PSP investigated the matter sufficiently, e.g. to identify that the consumer acted with gross negligence.

Question 10: Do you have any other comments on the information sharing requirement, taking into account the draft policy document at Annex 1 and the draft guidance at Annex 2?

Question 11: Do you have any additional feedback on the draft policy document at Annex 1 or the draft guidance at Annex 2?

Question 12: Do you have any additional suggestions for inclusion in the standard of care that PSPs can expect of consumers in relation to authorised push payments?

- As set out in the response to question 5, it is essential that there is a requirement for the customer to provide truthful information to the PSP at all times. The PSP cannot intervene and stop a scam taking place or otherwise provide redress after the fact if the customer obfuscates the situation by being untruthful or omitting information. We have seen by comparing a standard UK insurance policy (Bupa) that a requirement for the policy-holder to provide truthful information is standard practice in the insurance industry.

- For scams falling within the investment and/or cryptocurrencies scam, as part of the standard of conduct, there must be a requirement for the customer to have verified the status of the relevant firm using the FCA register. This is publicly available information and is **a register published by the FCA specifically for this purpose.**

- Proceeding with a payment that fails confirmation of payee should be a sign of gross negligence – the purpose of the scheme is to help customers verify the identity of the payee, and if they proceed regardless of confirmation that the payee is not the person they think they are, this must fail an appropriate standard of caution

- Delegation of remote access to a fraudster, either by sharing passwords or KYC documentation to allow the fraudster to set up an account in the victim's name must be a sign of gross negligence – this is core part of keeping safe online, especially for payments, and there must not be a scenario where this does not meet an appropriate standard of caution. It is standard under the PSRs 2017 that PSPs are not liable for unauthorised payments where a customer has e. g. shared their card details with a third party or has lost their wallet which has their PIN code on a post-it note next to their card. As above there must be some standard of caution that consumers are required to apply to prevent moral hazard.

Question 13: Do you agree that a standard to report a suspected APP scam to the police should not be included at this stage? Please provide reasons for your answer.

No.

Requiring a police report would align with the requirements in the EU Payment Services Regulation, and is important evidence that an actual fraud has occurred. It would also assist with data sharing to help police prosecute (especially as PSPs only have information on payments and not social media messages etc)].

Members of the EMA, as of September 2023

AAVE LIMITED
Airbnb Inc
Airwallex (UK) Limited
Allegro Group
Amazon
American Express
ArcaPay UAB
Banked
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network EMEA Limited
Boku Inc
Booking Holdings Financial Services International Limited
BVNK
CashFlows
Checkout Ltd
Circle
Citadel Commerce UK Ltd
Contis
Corner Banca SA
Crypto.com
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
Globepay Limited
GoCardless Ltd
Google Payment Ltd
HUBUC
IDT Financial Services Limited
Imagor SA
Ixaris Systems Ltd
J. P. Morgan Mobility Payments Solutions S. A.
Modulr Finance Limited
MONAVATE
MONETLEY LTD
Moneyhub Financial Technology Ltd
Moorwand
MuchBetter
myPOS Payments Ltd
Nuvei Financial Services Ltd
OFX
OKG Payment Services Ltd
OKTO
One Money Mail Ltd
OpenPayd
Own.Solutions
Park Card Services Limited
Paymentsense Limited
Paynt
Payoneer Europe Limited
PayPal Europe Ltd
Paysafe Group
Paysend EU DAC
Plaid
PPRO Financial Ltd
PPS
Ramp Swaps Ltd
Remitly
Revolut
Ripple
Securiclick Limited
Segpay

Skrill Limited
Soldo Financial Services Ireland DAC
Square
Stripe
SumUp Limited
Swile Payment
Syspay Ltd
Transact Payments Limited
TransferMate Global Payments
TrueLayer Limited
Trustly Group AB
Uber BV
VallettaPay
Vitesse PSP Ltd
Viva Payments SA
Weavr Limited
WEX Europe UK Limited
Wise
WorldFirst
Worldpay
Yapily Ltd