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

Ruth Evans
Chair
APP Scams Steering Group

15 November 2018

Dear Ruth

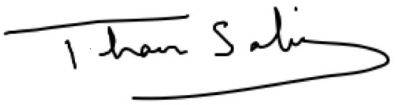
Re: EMA response APP Scams Steering Group Draft Contingent Reimbursement Model Code

The EMA is the EU trade body representing electronic money issuers and alternative payment service providers. Our members include leading payments and e-commerce businesses worldwide that provide online payments, card-based products, electronic vouchers and mobile payment instruments. They also include a large number of smaller Payment Service Providers, including startups. The majority of EMA members are authorized in the UK, and 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.

The issues raised in this response have significant competition and policy implications for our members. Implementation of the code in its current form could in our view lead to multiple failures of smaller PSPs, who would either be unable to compete with larger PSPs with more diverse sources of income, or be the subject of multiple fraud related compensation claims – over which they have no control, and which they cannot support. To this end, we counsel against extending the code beyond the meeting of a reasonable duty of care, and against a subjective definition of vulnerability. It is better to achieve a significant but incomplete protective environment for users than to seek to protect users perfectly and in doing so degrade the product offerings, increase costs for users and decrease choice.

I would be grateful for your consideration of our concerns and look forward to continuing this work.

Yours sincerely



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

EMA response to consultation

Q1: Do you agree with the standards set out in the Standards for Firms?

We broadly agree with the standards set out in the Standards for Firms.

However elements of the Standards are very difficult, if not impossible to implement by smaller and alternative fintech PSPs. In contrast with large credit institutions, an APP Scam reimbursement could have a significant damaging impact on the business of a smaller PSP.

On the other hand, PSPs that cannot sign up to the Code will be at a competitive disadvantage in relation to those who are able to do so, as consumers will perceive greater protection offered by larger PSPs, leading to the contraction of the market for smaller PSPs, less choice for consumers, and fewer low cost services.

We regard this as a significant anti-competitive issue, and whilst we accept that a duty of care to alert a customer with regard to a possible scam can exist, that a consequent reimbursement may be desirable, and that our members may wish to participate in such a code, we have serious concerns and objections with regard to the extent and circumstances of compensation. We do not accept that a wider compensation obligation arises in the different circumstances contemplated by the standards, nor that the PSP which is in no way responsible for the fraud, should be uniquely placed in the role of insurer or arbitrator.

This is exacerbated by the fact that the fraud takes place entirely outside of the domain of the PSP, and the PSP does not have any statutory investigative powers nor the know-how or resources to discover the nature or merits of the claim. This is entirely a matter for law enforcement and for government led action.

It is noted PSPs who are members of the EMA are principally specialist payment providers who are proscribed from lending the funds of users, and therefore are restricted in the income that they generate to transaction related income streams. As an example, if the total revenue generated by a PSP was in the region of 1% of the value of a transaction, from which its cost of doing business must be extracted, it would have to process at least 100 equivalent size transaction to recover the loss on a single claim of fraud. Once the costs of doing business are taken into account, this is likely to increase to perhaps 1000 or transactions. There are other sources of fraud, and other costs that also have to be borne. The impact on small PSPs may very well be catastrophic.

In the response that follows, we have commented on the provisions in more detail.

Separately, it is in the interests of all parties, particularly UK consumers, that an appropriate Code is widely adopted and results in a significant reduction of APP Scams. Careful consideration needs to be given to ensuring that the Standards for Firms or related evidential requirements are not so prescriptive that they result in lower rates of adoption of the Code by PSP's.

In particular, non-Bank PSP's should be able to commit to and comply with the Code without a mandatory requirement to participate in other industry codes, data sources, technologies etc which require financial commitments to participate in and/or significant operational integration

resources. For example the EMA believes that it is desirable that a start-up Fintech PSP commits to the code from launch without having to become a CIFAS member provided that it has effective on-boarding fraud controls in place.

Specific comments:

a. General Principles for Firms: GF

A PSP's ability to ensure compliance with GF 1(a) may be challenging where the PSP works with many different partners such as programme managers, who would be responsible for designing and running any educational or awareness-raising project. This is a common business model for card based e-money issuers. It may be difficult for the PSP to ensure compliance by partners with their educational obligations at *all times*, so we propose that for the purposes of an APP Scam reimbursement decision, compliance with GF 1(a) is a relevant consideration only for the programme under which that particular APP Scam has taken place.

b. Standards for firms:

SF1

We agree that firms should take reasonable steps to protect their Customers from APP fraud. However we do not agree with the requirement that firms provide a greater level of protection for customers who are considered vulnerable to APP fraud. PSPs mostly hold very little personal information on their customers, making it almost impossible to make a judgement regarding their customers' vulnerability to APP fraud. Staff of EMA members do not hold appropriate levels of training to be able to judge whether a customer is vulnerable to APP scams or not. This issue may be even more acute for start-up Fintech PSP's. It is therefore very unlikely, or in some cases impossible for a PSPs to provide a greater level of protection for customers considered vulnerable to APP fraud. It is more appropriate for PSPs to defer such a judgement to the FOS and reimburse customers retrospectively than to take on such a role themselves.

It is specifically troubling that the code suggests that PSPs identify vulnerability with respect to APP Fraud; an impossible task given the breadth of fraud hat is covered, the limited engagement with customers, the skillset of PSP staff as well as privacy and customer expectations.

We propose the deletion of the text below:

"Sending Firms should take reasonable steps to protect their Customers from APP fraud. This should include procedures to detect, prevent and respond to APP fraud. ~~Procedures should provide a greater level of protection for Customers who are considered vulnerable to APP fraud."~~

SF1(1):

PSPs conduct transaction-based analytics as a matter of course, and often use artificial intelligence to improve their systems. However, the reference in SF(1) to firms not only identifying payments, but also **customers,** that run a higher risk of being associated with APP Fraud is very difficult to implement in practice, as it is highly subjective, and relies on a much greater amount of data held on customers than alternative/smaller PSPs currently hold. Communication by alternative/fintech PSPs with the customers is primarily online, and often for one-off or occasional transactions, so they do not have the same one-to-one interaction over a phone or face-to-face that a high street bank might have. The nature of products that alternative/Fintech/smaller PSPs offer mean that customers are usually not willing to volunteer more than the basic mandatory information necessary to open the account and perform the transaction. Even in relation to online data, alternative PSPs may not have historical payment data, or information on other financial products held by that customer. The only data in this regard that a fintech PSP is likely to hold is where that customer has previously been victim to an APP scam with that same PSP.

This requirement will lead to PSPs being held liable for information they don't hold. E.g. a Payment I*nitiation Service Provider (*"PISP") offering services to a fintech providing person-to-person payment services will hold no information whatsoever to perform anti-fraud analytics (the fintech would potentially have the information in this case)

In the case of programmes targeting vulnerable consumers, such as the elderly, unbanked, or immigrant communities, the expectation could be very different. However in general it will be extremely difficult for PSPs to identify consumers that are more at risk of becoming a victim to an APP scam.

We therefore propose to remove the word "customer" from SF1:

"Firms should take appropriate action to identify ~~Customers and~~ payment authorisations that run a higher risk of being associated with an APP fraud"

SF1(b)

We propose the following minor amendment:

"Firms should train their **relevant** employees…"

SF1 (2)(c)

We agree that warnings should be risk-based. However this should not preclude firms from

issuing warnings to all new customers, for example, or for all new payees.

We are also supportive of solution driven warnings, and other controls like Confirmation of Payee (CoP) that will educate consumers and drive down the incidence of APP scams.

A key point to note in all the standards is that any effective warning loses efficacy if consumers are aware that they will be reimbursed regardless of their own actions. We do not expect a significant reduction in incidents due to customer due diligence if a no blame scenario is introduced. We are therefore opposed to a no-blame-no-blame reimbursement scenario.

Reimbursement of users in all circumstances simply puts money in the hands of fraudsters, provides no disincentive to users, and incentivises fraudsters to continue this practice.

SF1 (2)(d)

The guidelines must be payment channel neutral, and not require firms to suggest using a competitors service or a more expensive payment method. Many consumers will be paying via a channel that is specifically requested by the payee. It is for example expensive for small businesses to accept card payments, if these are the proposed alternative. It is also expensive for PSPs to fund chargebacks for card payments. This suggestion does not contribute to a shift in consumer behaviour towards making safer bank transfers, or to reduce the incidence of scams. It goes against the guiding principles of the steering group, to mitigate the risk of payment by bank transfer rather than to disincentives the use of this payment method.

Effective Warnings should focus on effective customer due diligence -- which is the key driver of much APP fraud.

SF1 (2)(e)

We agree with the provisions in relation to effective warnings. However we note that there may be a conflict between the amount of information expected to be presented to the customer in SF1 (2)(c), SF1(2)(d) and SF1(2)(e)iii, and the requirement that the warning be "impactful". If presented with too much information, consumers may just wish to click through without reading any of it. For example for app-based products, a quick and simple pop-up will be impactful but may not include all the recommended information set out in the Code.

SF1 (2)(e)v

For the reasons detailed above in relation to identifying vulnerability, we propose the following amendment, as the PSP may not have any data to categorise the customer type:

"Specific – tailored to the ~~customer type and the~~ APP fraud risk identified by analytics during the Payment Journey, and/or during contact with the Customer."

SF1 (4)

Vulnerable customer identification: we can use information such as age to determine if someone is higher risk, but questions of someone's financial capability are unknown without making arbitrary judgements and using invasive techniques. A third party, like the FOS, would be better equipped to judge a consumers vulnerability objectively and fairly, thus sparing consumers the requirement to share intimate information with their PSP. Such vulnerability should however be defined in an absolute sense and not in relation to each type of fraud or scam – that is an impossible requirement that cannot be delivered by any third party, perhaps even family members.

How would a PSP know if someone is vulnerable to a Romance scam? Or how is vulnerability to a purchase scam quantifiable?

For clarity, we are strongly against proposals that involve the PSP seeking sensitive user information that is unrelated to their business relationship with the PSP, or of encouraging PSPs to make value judgements about users.

We propose deletion of the APP Scam subjective element of vulnerability. Vulnerable customers in an absolute sense, can make themselves known to the PSP, who could then make provisions for a more appropriate delivery of the service. Otherwise, the FOS is able to address issue of vulnerability.

Application to PISPs: for clarity, these provisions should not apply to a PISP that has no knowledge of the payer, but would apply to the payer's account holding PSP.

SF1(4)(c)

The Code should not mandate PSP's to participate in other non-public codes such as BSI PAS 17271 as this is a costly exercise that is not required by financial services regulation; it would therefore likely reduce participation of non-Bank PSP's. We suggest the following change:

"industry standards, **for example** BSI PAS 17271"

SF1 (5)(a)

Whilst we understand the rationale behind the desire for firms to be able to delay payments, PSPs offering push payments are undertaking to execute immediately. This is set out in the PSRs, Guidance, and also in payment scheme rules. A firm that delays a payment for any reason other than a legal requirement will be taking on a significant risk.

This requirement places smaller PSPs at a disadvantage, as they are not resourced to provide 24/7 service. Large banks are able to take a risk-based approach towards blocking transactions, then calling the customer to check (or expect the customer to call the bank). However smaller PSPs cannot provide this level of customer service, so are unlikely to block transactions. The emphasis in the Code should be on effective warnings rather than an expectation that PSPs delay or block transactions.

If this provisions is carried, then further regulatory guidance on delaying payments that would consider all participants would be required.

Impact on PISPs: it is not generally technically possible for a PISP to delay an immediate payment for a significant amount of time.

SF1 (6)

The **Best Practice Standards** are helpful, but provide an additional layer of compliance; consideration should be given to making adoption of BPS non mandatory.

SF2(1)(a)

Non-Bank and Fintech PSP's often use sophisticated techniques of CDD. It is important that any evidential expectations are broad and capable of accommodating differing means of risk based

CDD.

When proving compliance with SF(1)(a) PSP's are restricted in the information that can be provided to the Sending Firm. An arbitration process is needed to facilitate this.

SF(1)(b)

For non-Bank and Fintech PSP's it is critical not to mandate participation in Bank led data sources such as CIFAS, and others. This will reduce participation in the Code and will be regarded as an anti-competitive provision by our members. We propose the following amendment:

"Firms should use available shared intelligence sources and industry fraud databases **or deploy other effective techniques** to screen Customer accounts..."

SF2 (3)(b)

We agree that firms should train employees involved in transaction monitoring to identify transactions at higher risk of being associated with an APP Scam. However not all staff need to be trained in this way. We propose the following amendment:

*"Firms should train their **relevant** employees on how to identify indicators of circumstances around, and leading to, transactions that are at higher risk of facilitating APP fraud."*

SF2(4)

As stated above, it should be possible for non-Bank PSP's to comply with the Code without mandating full Compliance with the Best Practice Standards in order to maximize adoption of the Code.

SF2(5)

Repatriation should be to the Sending Firm and not the Customer. Clarification on the arrangements when the Sending Firm does not participate in the Code would be helpful.

SF2 (5) (a)

PISP impact: please note that a PISP which is purely initiating payments cannot freeze any funds as they never pass into the PISP's bank accounts. Therefore, these obligations can only apply to banks and other ASPSPs.

R1

The provisions on residual risk/no blame scenario are currently expressed in the draft code (R1) as being reimbursed by the PSP, along with other circumstances giving rise to reimbursement.

However the Consultation Paper (see paragraphs 4.3 and 4.4) states that in the "no-blame" scenario, PSPs may *administer* a refund, but not that they would be expected to reimburse from their own pocket. The conditions at R2(a)-(g) do not currently distinguish no-blame as an exception to reimbursement. We propose to include "no-blame" in the list of exemptions from reimbursement, and then later include a statement that in the case of no-blame, PSPs can administer a reimbursement from another source (amending R3).

"*The Firm has met the standards expressed in the Standard for Firms, and the Firm cannot establish any one of the manners described in R2(1) (a) to (g) has occurred through an act or omission of the Customer."*

This then leaves the opportunity for the PSP to *administer* the reimbursement on behalf of a third party, to simplify the process for the consumer.

A provision can be made at R3 with a new paragraph (3):
"*(3) Once the firm has received confirmation of the bona fide nature of the claim from [the police], and has received payment from [the designated fund], it can assist by administering the reimbursement.*"

As the PSP has no investigative powers outside its own business relationship, and as the scam draws in other parties and activities, the role of investigating to ensure there is no first party fraud needs to be undertaken by a third party entity with such powers, such as the police.

R2(1)(g)

Guidance is required on how "grossly negligent" will be interpreted. Clear examples would be helpful

R2(3)

As set out earlier:

(i) It will be extremely difficult for all PSPs and particularly smaller PSPs to enquire of information required to assess vulnerability In relation to a particular type od scam

(ii) 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.

(iii) Even attempting such a feat would involve unacceptable intrusion into the lives of customers, and a skill set that is closer to psychology than to payment service provision, and resources that are not available.

(iv) There are considerable public policy implications in the field of privacy and personal data that would also merit consideration.

Impact on PISPs: note as PISPs do not come into funds, they should not be expected to administer or reimburse funds.

R4

We agree with the sentiment of R4, that the customer have access to redress as quickly as possible, we believe it is in the interests of customer, PSP and the FOS that due process is followed and a complaints process completed with the PSP before the customer approaches the FOS. This will ensure that the PSP is able to complete all internal investigation, and will reduce the workload for both the FOS and the customer when it comes to adjudicating the case.

FOS charging process: there is concern regarding the suitability of the current FOS charging process for complaints that originate from compensation claims arising from APP Scams. The current FOS process involves the firm paying a fee of £550 in relation to the administration of a complaint irrespective of whether the FOS finds in favour of the firm or against it.

This could create a de facto threshold of £550, below which it would be uneconomical for PSPs to refuse claims, even if they are unfounded or where the user has been grossly negligent.

We propose the following changes to the wording:

"Where a Customer has received a negative reimbursement decision ***and complained****, all the Firms involved will take all reasonable steps to* ***accelerate their internal complaints process to***

enable a Customer who is eligible and wishes to do so, to commence ~~immediately~~ the process of challenging that decision with the Financial Ombudsman Service ***as soon as possible***.

Furthermore, the FOS should give serious consideration to suspending the application of their fee, where a complaint is manifestly without merit, and the complainant to have pursued the complaint only as a means of forcing the firm's hand. This would be akin to the current treatment of vexatious complaints.

Q2: We welcome views on whether the provision that firms can consider whether compliance would have helped prevent the APP scam may result in unintended consequences - for example, whether this may enable firms to avoid reimbursing eligible victims?

We support the proposed provision in full, and do not believe it creates an incentive for firms to avoid reimbursing eligible victims. Its intention is not to create a loophole, but to introduce a natural balance to the Code.

The Code should incentivise PSPs to prevent APP fraud. It is reasonable to expect a PSP to reimburse the customer where they could have taken steps under their duty of care set out in the Code that would have prevented the scam from occurring. However, where the non-compliance has no bearing on whether or not the scam would have taken place, for example with GF(3) on customer aftercare, this should not lead to the firm being expected to fund the reimbursement to the customer. It is difficult to understand the rationale for applying irrelevant facts to justify liability/blame. Otherwise the Code simply creates an insurance policy penalising PSPs.

In any case, under the Code, "eligible" victims (i.e. victims considered to have met the Customer Standard of Care) will be reimbursed, whether by the PSP or the "no-blame" fund.

Q3: We welcome views on how these provisions (R2(1)(a) and (b)) might apply in a scenario where none of the parties have met their levels of care.

This will depend on the factors of each case.

For example, the duty of care would serve an end only if the customer is not grossly negligent. If he is, it would make no difference, and the PSP should not be required to send any money to the no-blame fund. Given fraud is perpetrated on the customer by a third party, the shortcoming is in detecting it, not a shortcoming that caused it. If a customer is reimbursed in such a case, they are not encouraged to take care the next time.

Q4: Do you agree with the steps customers should take to protect themselves?

Yes we agree customers should take these steps to protect themselves.

We propose elaborating on the standard consumers would be expected to meet, and to set out such guidelines and expectations in relation to 'too good to be true' offers or 'well known scam scenarios' etc.

We propose to amend R2(1)(d) to add: "and/or take reasonable steps to validate that a payment does not reasonably relate to a scam or fraud"

Q5: Do you agree with the suggested approach to customers vulnerable to APP scams? In particular, might there be unintended consequences to the approach? Are there sufficient incentives for firms to provide extra protections?

We do not agree with the suggested approach to customers vulnerable to APP scams.

The broad definition of vulnerability leads to an obligation to collect a wide range of data from customers to establish the degree to which they may be vulnerable, and more specifically, vulnerable to APP Fraud.

Whilst asking for information on background, physical and learning difficulties, 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,

This is again particularly detrimental to the business of alternative banking PSPs who tend to provide products on Mobile Apps, a key differentiating factor from traditional banks.

The definition of vulnerability should therefore be objective in broad terms (eg. a person with learning difficulties, or elderly or disabled in some manner) and not subjective to the particular fraud typology. Furthermore, the interpretation of the vulnerability could be product specific as well as user specific, so that PSPs could only be expected to solicit such information as would be reasonable in the context of their relationship with the user.

More extensively utilised products would canvass more information whilst single use products would warrant less. Provision should be made for PSPs to develop knowledge of customer behaviour over a period of time, and they should not be penalised for not collecting personal information at or immediately after onboarding.

For ease of reference, we have repeated below, points made on this issue in commentary on provision R2:

(i) It will be extremely difficult for all PSPs and particularly smaller PSPs to enquire of information required to assess vulnerability In relation to a particular type od scam

(ii) 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.

(iii) Even attempting such a feat would involve unacceptable intrusion into the lives of customers, and a skill set that is closer to psychology than to payment service provision, and resources that are not available.

(iv) There are considerable public policy implications in the field of privacy and personal data that would also merit consideration.

Q6: Do you agree with the timeframe for notifying customers on the reimbursement decision?

Yes the timeframe of 15 days is appropriate in most circumstances, with an extension to 35 days where the PSP communicates to the customer.

Q7: Please provide feedback on the measures and tools in the Annex to the code, and whether there any other measures or tools that should be included?

We agree with the measures included in the Annex. However we propose that the reference to the BSI Code of Practice be moved to the Annex, not the Code itself, as it is not a public document. It is not clear why this document should be included in the Code, whilst other reference documents are inserted in the Annex.

We note that some tools may require more time and resource to be implemented for smaller/alternative/fintech PSPs. For example, PSP business models that involve numerous partnerships such as with programme managers, who would be responsible for designing and running any educational or awareness-raising project. This is a common business model for e-money issuers. Allowance for some variation should be made, and each programme should be considered separately.

Q8: Do you agree that all customers meeting their requisite level of care should be reimbursed, regardless of the actions of the firms involved?

We agree in principle; with two significant caveats.

The consumer level of care needs to be defined in a reasonable manner, that does not offer reckless individuals the opportunity to avoid responsibility, or a safety net for taking chances that would not otherwise have been taken. This would result in an acceleration of fraud, in users opting for 'too good to be true' opportunities etc. The position in relation to pyramid schemes for example is also worthy of specific consideration, as it could give rise to widespread and system claims.

For clarity, where a PSP has met their level of care, the reimbursement should be funded from a third source, and NOT from the PSP. Furthermore, no PSP should be expected to provide liquidity or interim payment in this regard. This is particularly important in relation to smaller PSPs.

We also object to proposals for industry funded sources of reimbursement in such scenarios, and warn against any such proposals that act as an anti-competitive provision, favouring larger and better funded institutions – please also refer to our response to Question 10 below.

Q9: Do you agree that the sending firm should administer any such reimbursement, but should not be directly liable for the cost of the refund if it has met its own standard of care?

We cannot agree to this while there is uncertainty on key issues:

- How will the firm know that a user is eligible and not party to a first party fraud. It has no investigative powers, so what can it do to mitigate this risk?
- Given that it is not paying from its own funds, what process is there to implement controls over this process
- Is the firm the final arbiter or will its judgement be reviewed?

These issues need to be elaborated before a view on this can be reached.

Q10: **What is your view on the merits of the funding options outlined in paragraph 4.6? What other funding options might the working group consider?**

We do not support any form of PSP funding for the reimbursement of customer funds in a "no-blame" scenario.

The consequence is that PSPs will in effect provide an underwriting service for APP Scam fraud, offering compensation even if no fault can be shown (i.e. in the "no-blame, no-blame" scenario). For example, a failure in the security of an accountancy firm that allows hackers to substitute fake payment details, or poor oversight by a dating web site that allows scammers to perpetrate

widespread 'romance fraud' etc. would be regarded as shortcomings to be attributed to the PSP even if the PSP has met its requisite duty of care, detecting, preventing and responding to such risks.

This 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 and dating web site providers in the above examples, 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. This would also create a disadvantage for alternative/smaller PSPs, who have less ability to absorb additional costs than large banks, and would need to pass the costs on to consumers, thus making their product less attractive.

We see 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; and we ask that the ASSG make a similar distinction, and restrict compensation to the former.

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.

We support a government-funded scheme, as this would incentivize the government to bring all relevant parties together to address the issue.

Q11: How can firms and customers both demonstrate they have met the expectations and followed the standards in the code?

It will be difficult for the Financial Ombudsman to judge compliance with the Code in many cases, for example in relation to the transaction risk analysis conducted by a firm. We propose that FOS staff dealing with these complaints receive specially targeted training in coordination with the FCA, PSR and industry.

This should be transparent, should reflect a broad cross-section of industry, and should also result in an output that can be used to inform consumers and increase their awareness.

Q12: Do you agree with the issues the evidential approach working group will consider?

Yes we agree. We do however stress the need to ensure that evidential requirements are not slanted towards larger institutions such as large Banks so that they present a barrier to entry or significant operational challenge for smaller PSP's with different operating and business models.

Q13: Do you recommend any other issues are considered by the evidential approach working group which are not set out above?

Staff of EMA member firms do not hold appropriate levels of training to be able to judge whether a customer is vulnerable to APP scams or not. It is beyond the usual remit of a PSP's role to ascertain the level of vulnerability to an APP Scam.

Vulnerability should be defined objectively, and users encouraged to make such needs know. Other approaches result in unreasonable demands on firms and their staff, as well as unacceptable intrusion on customers.

Once vulnerability is defined objectively, users will also be able to rely on the judgement of the FOS where they fail to implement appropriate measures, and result in a failure of their duty of care.

Q14: How should vulnerability be evidenced in the APP scam assessment balancing customer privacy and care with the intent of evidential standards?

We do not agree with the suggested approach to customers vulnerable to APP scams.

We agree that firms should take a more sensitive approach towards customers considered to be vulnerable during an investigation, and where there are programmes or products specifically designed for groups that are vulnerable.

However the broad definition of vulnerability leads to an obligation to collect a wide range of data from customers to establish the degree to which they may be vulnerable, and more specifically, vulnerable to APP Fraud. Whilst asking for information on background, physical and learning difficulties, 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 for the PSP to solicit such detailed personal information. EMA members also express a high level of discomfort at making such a judgment, and staff are not trained appropriately to be able to do so. It is therefore very unlikely that a PSP will be able to evidence compliance with a requirement that firms provide a greater level of protection for customers considered vulnerable to APP fraud. PSPs are more to defer such a judgement to the FOS and reimburse customers retrospectively than to take such a role on themselves.

The evidence required of PSPs to demonstrate treatment of vulnerable customers should therefore be product specific as well as user specific, and PSPs should only be expected to solicit such information as would be reasonable in the context of their relationship with the user. More extensively utilised products

would canvass more information whilst single use products would warrant less. Provision should be made for PSPs to develop knowledge of customer vulnerability over a period of time, and they should not be penalised for not collecting such information at or immediately after onboarding.

Please also refer to our response to Question 5.

Q15: Please provide views on which body would be appropriate to govern the code.

Of the options set out in the Consultation Paper, Pay.UK appears to be the most appropriate body. However we note that there is very little to no representation of the alternative/small PSP view in the Pay.UK governance structure. Smaller providers are unable to deploy resources into such institutions and rely on their trade body for representation. The EMA is ready to discuss options in this regard.

In relation to management of the ongoing governance of the Code, we propose that – as the obligation to identify customers who are considered to be vulnerable to APP Scams is likely to be impossible for most alternative or small PSPs, and is the least tangible measure to introduce – this provision is removed from the initial CRM Code. The FCA is expected to consult on Guidance on their expectations in relation to the treatment of vulnerable consumers in early 2019. Once this Guidance has been adopted, it may inform the requirements set out in the CRM Code, leading to a Code that is achievable for smaller/alternative PSPs.

Q16: Do you have any feedback on how changes to the code should be made?

A review after a year seems reasonable, with regular reviews every few years thereafter. A further review should also be undertaken prior to PISPs being brought within scope.

In relation to management of the ongoing governance of the Code, we propose that – as the obligation to identify customers who are considered to be vulnerable to APP Scams is likely to be impossible for most alternative or small PSPs, and is the least tangible measure to introduce – this provision is removed from the initial CRM Code. The FCA is expected to consult on Guidance on their expectations in relation to the treatment of vulnerable consumers in early 2019. Once this Guidance has been adopted, it may inform the requirements set out in the CRM Code, leading to a Code that is achievable for smaller/alternative PSPs.

In relation to entities that may be permitted to propose changes to the Code, this should not be limited to signatories. There may be entities that wish to sign up to the Code, but are unable to do

so due to provisions that prevent their being able to comply. They should also be offered the opportunity to propose changes to the Code. This will encourage wide adoption of the Code.

Q17: Is a simple 50:50 apportionment for shared blame between firms appropriate? If not, what is a sensible alternative?

Yes this is appropriate.

However, as set out in SF of the Code, where the compliance with that standard would not have had a material effect on preventing the APP fraud that took place, PSPs should not be expected to bear 50% of the cost.

The Code should incentivise PSPs to prevent APP fraud. It is reasonable to expect a PSP to reimburse the customer where they could have taken steps under their duty of care set out in the Code that would have prevented the scam from occurring. However, where the non-compliance has no bearing on whether or not the scam would have taken place, for example with GF(3) on customer aftercare, this should not lead to the firm being expected to fund the reimbursement to the customer.

Q18: Would the ADR principles as adopted by Open Banking in section 7 of its Dispute Management System Code of Best Practice be an appropriate arbitration process for the code?

Yes these ADR Principles are appropriate.

As the Open Banking dispute management and arbitration process has been agreed amongst the CMA9 (and participating Third Party PSPs), this may be an appropriate starting point for disputes in relation to the APP scams process. The OB process is also intended to complement procedures adopted for FOS complainants so as to minimise impact on participants.

However, we note that the OB dispute management process is untested as yet.

We also note that the CMA9 members of the OBIE are currently funding the operation of the Dispute Management System process, and that the costs for individual cases that are referred for mediation/adjudication are to be apportioned equally between parties.

Q19 What issues or risks do we need to consider when designing a dispute mechanism?

We note that the OB dispute management process is untested as yet. There is a risk that there are issues that will not be identified until the process is used.

Q20 What positive and/or negative impacts do you foresee for victims of APP scams as a result of the implementation of the code? How might the negative impacts be addressed?

The requirements set out in the Code on PSPs in relation to identifying those vulnerable to APP Scams may lead:

- To consumers being labelled as "vulnerable" and perhaps not having access to services they might otherwise access.
- Fintechs to avoid taking on customers who are considered vulnerable to APP scams (if this is possible to identify at the outset at all).
- PSPs to begin asking intrusive personal questions when onboarding new customers

Furthermore, there is no Reasonable manner in which customers can be rationally labelled as vulnerable to different types of frauds, except in the a broad objective sense. The elderly may be vulnerable to fraud generally etc.

Q21 What would be the positive and/or negative impact on firms (or other parties) as a result of the implementation of the code? How might the negative impacts be addressed?

The quantum of compensation that is being proposed by the CRM is not calibrated to the shortcomings that gave rise to the loss, nor is it proportionate to the income that is derived by the PSP from transactions. This is a matter for concern in itself, but is of critical concern for smaller PSPs and in particular to Payment Institutions and Electronic Money institutions who offer specialist payment services, usually prepaid or 'pass through', and who do not derive a supplementary income from other financial products that attach to an account such as overdrafts, personal loans, insurance etc.

The income derived by EMA member institutions is usually restricted to that from the payment service itself, and will be limited in scope. It may be a fixed amount that is not related to the transaction size, or it may be a percentage, usually significantly less than 1% of the value of the transaction.

User compensation however is proposed for the entire principal value of the transaction. This means that when compensating a single transaction of £100, it will likely require 100 legitimate non-fraudulent transactions of the same value to be processed in order for the PSP to recoup the cost of the compensation that was paid out – assuming for simplification a 1% transaction income.

The position in relation to certain alternative banking solutions, where EMA member PSP's support Fintech Client/Programme managers, is even more acute as the PSP average revenue for these types of programmes can be in the order of 5 basis points so an APP Scam of £5,000 would have generated revenue of £2.50. Compensation of the principal value would require 2000 legitimate transactions to recoup the compensation.

It is important to also note that APP Scams can be operated by highly sophisticated origanised criminal groups that specifically and aggressively target a particular group of users (this happens by analogy to different types of PSP). As such small and market entrant PSP's could be effectively driven out of business due to compensation payable in relation to quite a short period of time during which the PSP mitigates the specific targeting and prevents further APP Scams.

This can happen irrespective of the strength of controls in place as organized crime groups can be highly innovative. The pattern is then that the APP Scam migrates to another user group that may be attached to another PSP. Non-Bank PSP's are far less able to cope with the Compensation relating to such targeting APP Scams than Banks due to their business models and length of trading during which reserves are built up.

In the absence of other revenue streams, smaller PSPs will be disproportionately impacted by the proposed Code, and their ability to compete as specialist payment service providers will be adversely impacted.

The impact is particularly acute for non-bank PSPs providing innovative alternative banking solutions in direct competition to traditional banks as specifically envisaged by PSD2. The business models of these organisations and cost structures are entirely different from traditional banks. An underwriting type compensation model is likely to drive many organisations out of the market for banking services and represent a highly significant barrier to entry for potential new participants.

We therefore ask for more time to be taken by the ASSG to develop a more nuanced approach to user compensation that is fair and effective for all parties concerned.

The cost of compliance with the Code is disproportionately higher for smaller/alternative PSPs, and the costs of not complying also significant in terms of lost business. Smaller PSPs will essentially be caught between a rock and a hard place. For example, the data that PSPs are being asked to collect in order to assist in the determination of whether a customer is vulnerable to an APP Scam may easily fall within the definition of "sensitive personal data" under the General Data Protection Regulation. This type of information would require significant overheads to collect,

store and process, even if it could actually be applied for the purpose for which it is being collected. We believe the objective is untenable.

Q22 Are there any unintended consequences of the code, particularly those which may impact on consumers, which we should be aware of?

The requirements set out in the Code on PSPs in relation to identifying those vulnerable to APP Scams may lead:

- To consumers being labelled as "vulnerable" and perhaps not having access to services they might otherwise access.
- Fintechs could avoid taking on customers who are considered vulnerable to APP scams (if this is possible to identify at the outset at all).
- PSPs would be required to ask intrusive personal questions when onboarding new customers
- An unrealistic expectation that sensitive personal data could enable PSPs to predict vulnerability in relation to specific fraud typologies

If PSPs are required to fund the cost of "no-blame" reimbursement payments, smaller PSPs may not be able to compete with the larger counterparts, and ultimately the wider body of consumers will shoulder this cost.

Onerous obligations and evidential requirements which are not suitable for non-Bank PSP's will adversely impact such PSPs; FOS decisions based on compliance with these requirements will exacerbate the problem and the ultimate outcome could be an environment that reduces consumer choice and increases costs to consumers.

We counsel the reviewers to consider our submission carefully and to take the points made seriously. It is better to achieve a significant but incomplete protective environment for users than to seek an overly ambitious arrangements that cannot be achieved in practice and that undermines the positive results that have emerged.

Q23 How should the effectiveness of the code be measured?

The effectiveness of the Code can be measured be collecting data in relation to SF1 and SF2, and comparing it to similar data in one year, and on an ongoing basis thereafter. Specifically:

- Total value and volume of APP payments
- Proportion (by volume and value) of APP payments that were scam payments
- Of those scam payment, % of payments (volume and value) where the funds were frozen and repatriated.
- Number of claims made, divided by reimbursement outcome
- Categories of firms in each case should also be shown

This data could be separated into payments sent and payments received in order to determine the relative effectiveness of the requirements for sending and receiving PSPs.

It could also be separated by type of scam according to the scam types set out in the Annex to the Consultation Paper. This would allow for tracking of fraud trends.

List of EMA members as of November 2018:

Airbnb Inc
Allegro Group
American Express
Azimo Limited
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network Ltd
Boku Inc
CashFlows
Circle
Citadel Commerce UK Ltd
Coinbase
Corner Banca SA
Curve
Ebanx
eBay Sarl
Epayment Systems Ltd
Euronet Worldwide Inc
Facebook Payments International Ltd
First Rate Exchange Services
Flex-e-card
Flywire
GoCardless Ltd
Google Payment Ltd
IDT Financial Services Limited
Imagor SA
Intuit Inc.
Ixaris Systems Ltd
Merpay Ltd.
MuchBetter
Mypos.eu
Nvayo Limited
One Money Mail Ltd
Optal
Ozan
Park Card Services Limited
Paybase Limited
Paydoo
Payoneer
PayPal Europe Ltd
PayPoint Plc
Paysafe Group
PPRO Financial Ltd
PrePay Solutions
QIX Ltd
R. Raphael & Sons plc
Remitly
SafeCharge UK Limited
Securiclick Limited
Skrill Limited
Starpay Global Ltd.
Stripe
Syspay Ltd
Transact Payments Limited
Transact24 (UK) Ltd
TransferMate Global Payments
TransferWise Ltd
TrueLayer Limited
Trustly Group AB
Uber BV
Valitor
Vitesse PSP Ltd
Viva Payments SA
Wave Crest Holdings Ltd
Wirecard AG
Wirex Limited
Worldpay UK Limited
XCH4NGE LTD