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

Lending Standards Board
5th Floor Abbey House,
74-76 St John Street,
London EC1M 4DZ
By email: crmcode@lstdb.org.uk

7 October 2020

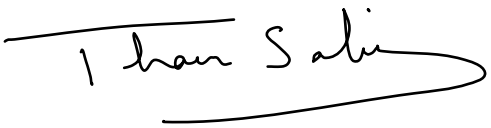
Dear Sirs

Re: Review of the Contingent Reimbursement Model Code for Authorised Push Payment Scams: consultation document; July 2020

The EMA is the EU trade body representing electronic money issuers and alternative payment service providers. Our members include leading payments and e-commerce businesses worldwide, providing online payments, card-based products, electronic vouchers, and mobile payment instruments. Most members operate across the EU, most frequently on a cross-border basis. A list of current EMA members is provided at the end of this document.

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

Yours sincerely,



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

Response

IMPLEMENTATION

Question 1: To what extent do you agree or disagree that the current version of the Code is clear about its purpose and scope?

EMA response:

Purpose

We agree with the overarching purpose of the Code, namely, that firms should take reasonable steps to protect their customers from APP scams.

Scope

With respect to scope, we propose the purchase scams be expressly removed from falling within the scope of the Code.

Purchase Scams pose specific challenges to PSPs: transactions that are the subject of a purchase scam are difficult to detect using traditional fraud control methods, as many indicate normal spending levels and patterns.

It is often difficult for firms to detect whether the scam is in fact a civil dispute instead. UK law already provides recourse for consumers in this context. Therefore, as the Code is designed to improve controls, offer vulnerable customers protection and offer a fallback for users who are being exploited by highly sophisticated criminals and scams, we propose that purchase scams are removed from the scope of the Code.

Question 7: What changes to the Code, or alternative options, should be considered to ensure that the protections offered by the Code can be applied to as broad a range of firms as possible?

EMA response:

The Code has been in force for over a year now and it is evident from the limited range of signatories (i.e. big banks with significant resources) that this is the case.

There are elements of the Code that are disproportionate for non-banks to comply with. EMIs in the UK offer a broad range of products, many of which preclude them from having a significant APP scam risk in comparison to the major CMA 9 banks e.g. an EMI may deal in cross border payments, or offer wallets for specific circumstances that are not used for day to day expenses. There are also elements that are simply too onerous for smaller PSPs to comply with. We suggest the adopts a proportionate, risk-based approach when considering the application of the Code to non-banks in the UK.

Below we set out which aspects of the Code are precluding smaller PSPs from signing up.

The main changes that need to be made to the Code to allow non-bank PSPs to sign up are:

1. To remove the requirement to identify vulnerable customers prior to a scam taking place; and

2. To allow firms who have conformed to the Standards for Firms to choose not to reimburse a customer (with the exception of vulnerable customers).

1. Definition of "Vulnerable" and Vulnerable customer to be identified *following* a scam

In summary:

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

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

(i) define vulnerability objectively, in broad terms (e.g. a person's age) and not subjectively with reference to the particular fraud typology. This will allow a PSP to assess whether a customer is vulnerable against certain criteria and ultimately ensure that customers who are genuinely vulnerable are assessed as such in every instance; and

(ii) alter the timing of the PSP's assessment of vulnerability, namely, require the assessment to take place once the customer has reported an APP scam to the PSP.

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

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

It would be more feasible and therefore allow more PSPs to participate in the Code if the process of collecting information and assessing whether a customer was vulnerable took

place following reports of a scam and that this assessment was with reference to objective criteria.

Finally, on this point, we would also appreciate clarification as to what basis a PSP may collect and process personal data that may indicate vulnerability. Assessing whether a customer is vulnerable may involve, in some instances, assessing their health and mental capacity. Therefore, it is likely that a PSP will be required to collect and process personal data concerning a customer's health from time to time.

Under article 9(1) of the GDPR, processing of special category data is prohibited unless a derogation applies. Special category data is personal data, amongst other things, that concerns a person's health. Unless a derogation is available, a PSP will not be able to collect and process such data. We would appreciate if the Code could expressly clarify the derogation a PSP may rely on in this instance.

2. No obligation to reimburse where the firm's conduct conforms to the appropriate standard

We suggest that where a PSP meets its standard of care under the Code, there should be no obligation to refund the customer:

In practice, the Code sets out a duty of care in relation to PSPs and expects them to compensate users in the event that they do not meet the standard set in the Code. The Code however does not distinguish situations where the PSP has met its requisite duty of care from those where it has not. R1 appears to require PSPs to compensate users who have suffered a loss irrespective of whether or not the PSP had fulfilled its duty.

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. 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 website 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.

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.

Position supported by common law principles

The position detailed above, namely, a person is not liable when they have upheld the requisite standard of care is based on well-worn precedents of common law. It is therefore a sufficient basis upon which to base the Code.

To explain further, at common law, where a person's actions conform to the required standard of care, they are not held liable. Similarly, here, if a PSP conforms to the standard of care set out in the Code, it should follow that the PSP should not be liable to reimburse the customer (with the exception of vulnerable customers).

The central principle to reimburse the customer following an APP scam stated in R1should follow these basic common law rules. We propose amending R2(1) as follows:

Current language: *A Firm may choose not to reimburse a Customer if it can establish any of the following matters in (a) to (e). The assessment of whether these matters can be established should involve consideration of whether they would have had a material effect on preventing the APP scam that took place.*

Proposed language: *A Firm may choose not to reimburse a Customer if it can establish that it met the standards set out in the Standards for Firms.*

New line: Where a Firm cannot establish that it met the standards set out in the Standards for Firms, the Firm may choose to not reimburse a customer or may choose to proportionally reduce a customer's award, if the Firm can establish any of the matters in (c) to (e) [using current lettering].

Letters (a) and (b) do not appear in the new proposed version of the text because a Firm conforming to the applicable Standards for Firm will have already:

(a) provided Effective Warnings in accordance with SF1(2); and

(b) implemented Confirmation of Payee functionality.

To explain the proposed language further, the exceptions set out in R2(1)(c) to (e) could be used in cases where the Firm did not conform their conduct to the Standards for Firms. For example, at common law, a person who has not conformed to their required standard of care can reduce their liability by asserting that the claimant also did not discharge their own standard of care (i.e. they also acted unreasonably).

This appears to be the intention of the exceptions to reimbursement listed in R2(1)(c) to (e).

In (c), the customer has, in short, proceeded with the payment without a reasonable basis for believing that (i) the payee was the person they expected to pay, (ii) the payment was for genuine goods or services, or (iii) the person or business with whom they transacted was legitimate. In other words, the customer has acted unreasonably.

R2(1)(d) further provides an example of where a customer has not conformed to their required standard. A reasonable micro-enterprise or charity would follow its own internal procedures to approve payments.

R2(1)(e) is direct and asserts that a firm may choose not to reimburse where a customer has been grossly negligent. This is clearly another example of a customer not conforming to the standard of conduct they are expected to.

Question 8: If you are a firm that has not signed up to the Code:

a) What is it that has prevented you from signing up to the Code?

b) What changes would need to be made for you to consider signing up to the Code?

1. Proportionality of the requirements

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

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

These include:

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

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

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

2. Uncertainty around liability assessments

There are a number of uncertainties around the scope and extent of firms' liability in the event of a scam, creating a barrier to entry for smaller PSPs. Whilst firms may be able to meet the majority of technical and operational requirements set out in the Code, we understand that the FOS appears to be interpreting the Code in a different manner from the LSB and even the PSR. This lack of clear guidance and uncertainty creates a barrier to participation. The impact is felt much more by PSPs that offer payments as service, as they do not benefit from the cross-subsidisation afforded by banks. In order for non-bank payment firms to join the Code, it is crucial that a clear liability framework is developed, and a sensible balance struck between protection for customers where the PSP has failed in their duty of care, and where an individual has authorised a payment, with all possible information provided and support offered by the PSP.

PREVENTION MEASURES

Question 18: Are the expectations of the sending and receiving firms, so far as they relate to effective warnings, clear? If not, what further clarity should be provided?

EMA response:

We agree that providing warnings can be effective. However, we note two issues arising from the Code as currently drafted:

(i) There may be a conflict between the amount of information expected to be presented to the customer 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.

(ii) Whilst it may be operationally feasible for PSPs to give warnings to customers in certain contexts, for example, a pop-up message during the course of setting up a new payee, it is not operationally feasible for PSPs to provide warnings that are "specific" and tailored to the customer type and APP scam risk identified by analytics during the payment journey.

Question 20: Do you have any views on whether CoP will improve the prevention of scams for customers?

EMA response:

We consider CoP will improve the prevention of some APP scams. In fact, effective CoP tools may also serve multiple functions for EMA members and their customers, in addition to scam protection.

However, it must also be recognised that not all APP fraud/scams will be caught by an effective CoP system:

APP Fraud Types & CoP

Common Scam Journey	2018 Q1 average value	2018 Q1 volume	2018 Q1 total scammed	% of 2018 Q1 total scammed	Mitigated by CoP?	Conditions for CoP to be effective
Invoice and mandate scam / conveyancing scam	£16,798	1128	£18,947,593	31%	Yes No	✓ Name on fraudulent account must be different to that of the intended payee for CoP to be effective (**NB**: this will place a reliance on PSP KYC processes at account opening) ✓ The payer must act on the warning message given by their PSP in response to a CoP request ✓ Implementation of an additional personal/business account check in CoP may strengthen effectiveness × If victim is led to believe the name on the fraudulent account is correct, then CoP will not be effective × Potential for MO to change due to complexities related to invoice factoring/discounting
Investment	£16,483	621	£10,236,211	17%	No	× Straight investment scams would not be mitigated by CoP, in particular for cases where the victim is led to believe the name on the fraudulent account is correct × **NB**: Implementation of an additional personal/business account check in CoP may make it effective in some cases
Impersonation – police/bank (caller from Fraud department)	£10,758	851	£9,155,068	15%	Yes No	✓ Name on fraudulent account must be different to what the payer expects for CoP to be effective ✓ The payer must act on the warning message given by their PSP in response to a CoP request × If victim is led to believe the name on the fraudulent account is correct, then CoP will not be effective × MO is likely to change once CoP goes live
Purchase scam (including rogue trader)	£956	9208	£8,805,408	14%	Yes No	✓ Name on fraudulent account must be different to what the pater expects for CoP to be effective (e.g. if a fraudulent website is impersonating a legitimate website) ✓ The payer must act on the warning message given by their PSP in response to a CoP request × Any purchase scams involving the victim making a payment by card or cash will not be mitigated by CoP (out of scope) × If victim is led to believe the name on the fraudulent account is correct, then CoP will not be effective
Impersonation – other	£6,525	942	£6,146,706	10%	Yes No	✓ Name on fraudulent account must be different to that of the intended payee (i.e. the person or entity being impersonated) ✓ The payer must act on the warning message given by their PSP in response to a CoP request × If victim is led to believe the name on the fraudulent account is correct, COP will not be effective × MO is likely to change once CoP goes live
CEO fraud	£20,841	162	£3,376,322	5%	Yes No	✓ Name on fraudulent account must be different to what the payer expects for CoP to be effective ✓ The payer must act on the warning message given by their PSP in response to a CoP request ✓ Implementation of an additional personal/business account check in CoP may strengthen effectiveness × MO is likely to change once CoP goes live
Romance scam	£10,971	254	£2,786,525	4%	Yes No	✓ CoP may be effective if the name on the fraudulent account is different from what the payer expects, and raises red flags about the true identity of the fraudster × MO is likely to change once CoP goes live
Advance fee	£1,442	1527	£2,202,340	4%	No	× Advance fee scams would not be mitigated by CoP

Question 21: Do you have a view on when the SF1(3), the provision on CoP, should become effective within the Code?

EMA response:

Phase 2 of Confirmation of Payee, which would allow indirect PSPs to join the scheme, will not be in place until 2021 at the earliest. Certainly, PISPs won't be able to join for some time, so the CoP provision should at least make allowances for firms who can't sign up due to technical barriers.

RESOLVING CLAIMS

Question 25: Are there any changes to the Code that could be made that would improve the process of reimbursing customers?

EMA response:

We agree with the sentiment of R3(2), that the customer have access to redress as without undue delay, 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.

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.

Question 27: Are the current principles for covering the cost of reimbursing customers appropriate, including in a scenario where both the sending and receiving firm have met their obligations under the Code?

EMA response:

No. Please see response to question 1. We suggest that where a PSP meets its standard of care under the Code, there should be no obligation to refund the customer.

Question 28: Should the Code continue to reference the no-blame fund as the means by which firms should recoup the cost of reimbursing a customer in a no-blame scenario?

EMA response:

No. Firms may wish to employ other methods of funding no-blame reimbursements. However, a centralised no-blame fund may still be of value for smaller PSPs who may not wish to carry the risk of having to reimburse a high value APP fraud.

As indicated in our response to question 7, a position following principles already set down in law would allow a firm to elect not to reimburse a Customer where the firm can establish it met the standards set out in the Standards for Firms in the Code. However, there are still likely to be 'no blame' cases even within that application of the Code e.g. if a customer is vulnerable, and a firm has met their prerequisite standard of care, the customer is arguably entitled to reimbursement.

One previous proposal to fund the “no blame” fund was for all FPS participants pay an additional fee levied on a per transaction basis. This proposal overlooked the different business models of various participants, and would have led to low risk firms - many of whom by virtue of their business model or product type witness insignificant volumes of APP scams – disproportionately contributing and thereby partially subsidising the other signatories (major banks).

While we agree with the principle that if a firm has conformed to the appropriate standard of care, the firm should not be liable for the loss sustained by the customer as a result of a scam, the previous proposals, such as the FPS levy, were not equitable.

Question 29: Should the Code be amended to accommodate other options for funding the reimbursement of customers in a no blame scenario? If so, what options should be accommodated?

EMA response:

Yes. Some firms prefer to self-fund their no-blame reimbursements.

Alternatively, the LSB may consider a cross-sectoral fund made up of contributions from outside the financial services industry, for example from entities who may have enabled the scam to take place through a data breach or ineffective KYC on merchants, or who could do more to prevent such scams by educating their customers.

If the Code holds only financial institutions responsible for a fraud that may have been prevented by other players, for example e-commerce platforms that onboard scam merchants, the non-financial services industry will lack an incentive to take action against these actors. We would support an attempt to bring wider industry to the table when it comes to funding reimbursements for fraud that EMIs and other financial services providers have already taken appropriate steps to prevent.

Members of the EMA, as of October 2020

AAVE LIMITED
Account Technologies
Airbnb Inc
Airwallex (UK) Limited
Allegro Group
American Express
Azimo Limited
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network Ltd
Boku Inc
CashFlows
Ceevo
Circle
Citadel Commerce UK Ltd
Coinbase
Contis
Corner Banca SA
Crypto.com
Curve
eBay Sarl
ECOMMPAY Limited
Em@ney Plc
ePayments Systems Limited
Euronet Worldwide Inc
Facebook Payments International Ltd
First Rate Exchange Services
FIS
Flex-e-card
Flywire
Gemini
Globepay Limited
GoCardless Ltd
Google Payment Ltd
IDT Financial Services Limited
Imagor SA
Ixaris Systems Ltd
Modulr FS Europe Limited
Moneyhub Financial Technology Ltd
MuchBetter
myPOS Europe Limited
Nvayo Limited
OFX
OKTO
One Money Mail Ltd
OpenPayd
Optal
Own.Solutions
Park Card Services Limited
Paydoo Payments UAB
Paymentsense
Payoneer
PayPal Europe Ltd
Paysafe Group
Plaid
PPRO Financial Ltd
PPS
Remitly
Revolut
SafeCharge UK Limited
Securiclick Limited
Skrill Limited
Soldo Financial Services Ireland DAC
Stripe
SumUp Limited
Syspay Ltd
Token.io
Transact Payments Limited
TransferMate Global Payments
TransferWise Ltd
TrueLayer Limited
Trustly Group AB
Uber BV
Vitesse PSP Ltd
Viva Payments SA
WEX Europe UK Limited
Wirecard AG
Wirex Limited
WorldFirst
WorldRemit