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

27 May 2021

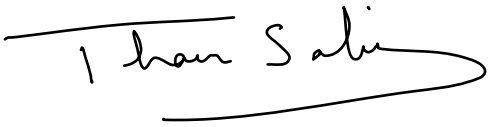
Dear Sirs

Re: LSB Call for Input for the CRM Code issued by the LSB

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

1. Please tell us about any APP scams which you have encountered, and which you perceive do not fit into the Code adequately?

a. Please describe the nature and volume of such scams.

Purchase scams (i.e. where a scammer poses as a merchant promising to deliver goods on receipt of payment) do not adequately fit into the Code.

b. Were Code provisions applied to such cases? If so, please describe how Code provisions were applied and describe any other aspects of the Code which impacted on such cases.

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.

With respect to the following paragraphs at Section 4.4(a) of the Review:

"*There was considerable feedback from financial service respondents who called for the* ***exclusion of purchase scams*** *from the Code, stating that* ***they take a disproportionate amount of time to assess****, are typically for* ***lower value*** *payments, yet are resourced by skilled fraud teams, and time spent on such cases can distract from more focused attention on customers who have suffered* ***larger monetary losses****."*

"***We were not persuaded that purchase scams should be excluded*** *from the Code simply on the basis that* ***they represent the highest volume of cases being assessed****. We are of the view that the level of care and focus given to a customer who has become a victim of a scam is a matter of after-care policy, and not a reason to exclude scams from the scope of the Code. It is the nature of a scam and a customer's circumstances at the time of the scam which should be in consideration when assessing any claim, as opposed to the monetary sum of the loss.*"

Please note that we have not previously taken the position that purchase scams should be excluded from the Code because "they take a disproportionate amount of time to assess". As stated above in the response to this question, we consider purchase scams should be excluded because (i) such scams are difficult to detect using traditional fraud control methods; and (ii) such transactions may not be scams but may instead be a civil dispute (and are therefore not appropriate to be assessed under the Code).

c. Do you have views on how the Code should be amended to help the prevention of such scams or mitigate their impact?

As the Code is designed to improve controls, offer vulnerable customers protection and offer a fall-back 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.

2. Are you aware of any resolution that was sought by the victims of such scams? How did they go about this? What was the outcome?

The outcome should be that the customer enforces their extensive consumer rights available under UK law by pursuing the merchant or platform where the sale of goods took place, or, alternatively by pursuing the merchant in the Small Claims Track or through Money Claim Online.

3. Do you have views on whether there should be a priority amongst firms with regards to Code participation? Please explain your view.

a. Are there other business models not mentioned to whom the Code would be of relevance?

Code participation is skewed in favour towards big banks (i.e. the existing participants – the CMA9) because there are elements of the Code that are too onerous for smaller PSPs to comply with. Non-bank PSPs, such as EMIs, offer a broad range of products in comparison to banks. An EMI's broad product range may preclude them from having a significant APP scams 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 too onerous for smaller PSPs to comply with. The LSB should look to adopt a proportionate, risk-based approach when considering the application of the Code onto non-banks in the UK. 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.

Further, we note the LSB's recommendation in Section 4.1(d) (Scope of the Code: business models) of the Review: "*The Code should recognise the wider range of participants within the payments industry while ensuring that it retains a consistent approach to the standards of protections provided.*"

And subsequent proposal to address this issue: "*The LSB will undertake a programme of engagement with firms providing payment services and PISPs to build on our understanding of the challenges faced by some participants in adopting the Code in its current form. This will be used to inform our work to allow for a broader application and adoption of the Code."*

We further note the reference to PISPs and their potential participation in the Code at Section 4.3(a) of the Review: "*We are also mindful of the* ***increasing range of participants*** *and diversity of business models within the payment journey,* ***such as PISPs****. Open banking has enabled customers to make payments via authorised PISPs rather than directly with their bank. This means that* ***responsibility for providing any warning would sit outside of Code signatories' control****. […] While PISPs currently sit outside of the Code, as set out above, their integration with the CRM Code is an area which* ***we will be exploring with a view to widening participation in the Code*** *and we will consider this issue alongside this specific workstream*."

The Code, as currently drafted, is not feasible for PISPs to participate. PISPs do not come into the flow of funds and PISPs, in certain circumstances, have limited visibility of the parties to a transaction. Accordingly, PISPs would not be able to feasibly comply with the majority of provisions in the Code and it would not be proportionate to levy liability for reimbursement on PISPs. If the scope of the Code were to be widened to allow PISP participation, numerous provisions would have to be excluded and new provisions drafted to legislate for the PISP business model. We would be happy to engage with the LSB on this point and highlight the main issues for PISPs with respect to the Code.

4. If you are a non-signatory firm, please tell us about your business model and your inclination to be a signatory to the Code.

There are currently no EMIs signatories to the Code. This may indicate that EMIs do not consider the Code, in its current form, appropriate for EMIs.

a. Are there additional barriers to the ones cited above that we should be aware of?

The main barriers to entry deterring EMIs from participating in the Code are:

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

2. that liability attaches to the PSP even in cases where the PSP's conduct has conformed to the Standard for Firms; and

3. the Code creates a significant compliance burden.

With respect to identifying vulnerable customers prior to a scam taking place:

- 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.

Please note that under the UK 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.

Liability attaching when the PSP's conduct has conformed to the Standard for Firms

With respect to liability attaching in cases where the PSP's conduct has conformed with the Standard for Firms, where a PSP meets its standard of care under the Code, liability should not attach.

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. The Code requires 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. 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.

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.

The Code obligation to reimburse the customer following an APP scam should follow these basic common law rules and apply only in cases where the PSP has not met the appropriate standard of care.

Significant compliance burden

Many EMA 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 are not 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 suggest that these provisions are either removed or curtailed for non-bank PSPs; we consider it is sufficient for a non-bank PSP to comply with their relevant governance obligations arising out of payment services or e-money regulation.

b. If so, what changes to the Code would be needed to accommodate your business model?

With respect to identifying vulnerability prior to a scam taking place, we propose to amend the Code to allow PSPs to assess whether a customer is vulnerable following a scam.

With respect to liability attaching to the PSP in cases where the PSP has conformed to the Standard for Firms, 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.*

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.

With respect to the issues we have raised regarding a significant compliance burden, we propose the Code be amended to allow firms to implement compliance measures on a risk-based approach.

4.2(a) APP scams data

We further note the LSB's recommendation in paragraph 4.2(b) of the Review: "*Work should be undertaken to ensure that there is a consistency of approach and interpretation to APP related data.* ***Data reporting requirements should be built into the Code*** *to support and inform the LSB's oversight work*".

And subsequent proposed measure to address the recommendation: "*We will work in collaboration with industry and experts to standardise definitions and measures for the Code to allow for greater consistency in CRM Code data.* ***We will build in a data reporting requirement into the governance and oversight provisions*** *outlined earlier in the report*."

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

The EMA does not support measures that are designed to "name and shame" PSPs into accepting liability for an APP scam (a liability they would otherwise not incur under law). "Shaming" is an ineffective tool to compel compliance, and will likely not reduce the incidence of APP fraud. Any data collected from PSPs in furtherance of this measure should be published in aggregate form. In addition, publishing data organised by individual firms may affect payment service users' rights with respect to their personal data. Accordingly, any data published as a result of this measure must be in aggregate form.

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

whether strong customer authentication was applied to the payment and any relevant exemptions.

The LSB may wish to liaise with the FCA to obtain data from the existing REP017 in order to elicit the information they are after rather than imposing a separate reporting obligation on firms.

c. If these changes were addressed, how likely are you to become a signatory?

These changes would make the Code fairer and more proportional; qualities which are essential prior to any EMIs considering signing up to the Code.

7. Are there any changes to the Code you believe would help to resolve any imbalances in sending or receiving firm responsibilities?

Apart from a potential imbalance between sending and receiving firms, we consider there to be an additional imbalance between large banks and non-bank PSPs. Until that imbalance is resolved, joining the Code will not be feasible for non-bank PSPs, such as most EMIs. One of the main issues creating this imbalance is the compliance burden associated with joining the Code as discussed in our response to question 4(a) above.

We note the LSB's recommendation in paragraph 4.1(e) of the Review: "***New governance and oversight provisions should be introduced into the Code****. These will require firms to have appropriate processes, controls and governance arrangements in place, ensuring that there is effective senior management oversight of the firm's adherence to the requirements of the CRM Code*".

And subsequent proposed measure to address the recommendation "***We will undertake work to develop new Code provisions*** *which reflect the approach taken to the Standards of Lending Practice. The new provisions and a timeline for implementation will be shared with firms in due course.*"

Please note that increasing the compliance burden on Code signatories will not entice non-signatories to join. PSPs (whether bank, EMI, payment institution, PISP etc.) are already subject to significant governance requirements. For example, a payment institution is already required under the Payment Services Regulations 2017 (as amended) ("**PSR**") to have in place the following as a condition of authorisation:

> (a) robust governance arrangements for its payment service business, including a clear organisational structure with well-defined, transparent and consistent lines of responsibility;
>
> (b) effective procedures to identify, manage, monitor and report any risks to which it might be exposed;
>
> (c) adequate internal control mechanisms, including sound administrative, risk management and accounting procedures, which are comprehensive and proportionate to the nature, scale and complexity of the payment services to be provided by the institution. [PSR 6(6)]

Additionally, a payment intuition is also required to carry out audits [PSR 24], comply with the list of conditions with respect to its outsourcing arrangements as well as notifying the FCA of an outsourcing arrangement [PSR 25], keep records for 5 years [PSR 31] and remain ultimately liable for the conduct of any entity to which they outsource activities [PSR 36].

The EMA could support the introduction of provisions requiring signatories to train staff in the Code in addition to awareness of APP scams, as this would be beneficial to payment service users; however, we could not support additional (to the PSR) and thereby unnecessary governance requirements.

9. Do you have views about how consumers understand their responsibilities and rights when they are undertaking a payment, particularly in circumstances involving more complex payments (e.g. including PISPs)?

a. Who do scammed consumers contact in such circumstances? If you have examples of where consumers have interacted with different firms after reporting a scam, please share with us.

Consumers are directed to their bank or – in the case of a suspected purchase scam - to the relevant merchant to resolve their dispute in the first instance.

10. What roles do you think organisations representing consumers who have been scammed, can play in the payment supply chain? Please outline any barriers and enablers you see to such roles.

Whatever heightened role is afforded to organisations representing consumers, in the interests of fairness, organisations representing PSPs should be afforded the same rights.

11. Do you have views on how Code responsibilities should be attributed along the payment journey?

It is not proportionate for all responsibility for an APP scam to be levied on the PSP. An APP scam is not confined to the payment journey – it begins much earlier than any payment taking place. An APP scam begins when a scammer initially targets and engages a victim.

We note the following statement at Section 4.3(d) of the Review: "*It was proposed that enhanced **scam risk customer messaging could appear on platforms** where there is a high propensity to scammer focus, **such as dating websites**, HMRC or other governmental departments, or via organisations that provide critical illness patient and family support. We have considered these suggestions carefully and we are of the view that this type of work **is outside of the remit of the LSB**, as we do not work directly with consumers*."

Platforms such as dating websites create an environment for fraudsters to carry out their scams with no liability to the platform. By omission, such platforms are arguably facilitating scams. Conversely, PSPs actively take measures to prevent scams, yet are burdened with liability. Why is it appropriate to levy liability on PSPs and no liability on the platforms where such scams take place? Platforms should not be able to escape liability and/or the

compliance burden on implementing scam-preventing measures merely because “this type of work is outside of the remit of the LSB”.

If the LSB consider it outside their remit to require platforms such as dating websites to take measures to reduce APP scams, the LSB could consider engaging the PSR or CMA to utilise their competition powers to compel platforms to implement such measures.

Members of the EMA, as of May 2021

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