Electronic Money Association
Crescent House
5 The Crescent
Surbiton
Surrey
KT6 4BN
www.e-ma.org

Duncan Hames
Director of Policy and Programmes
Transparency International UK ("**TI**")
10 Queen Street Place
London
EC4R 1AG
United Kingdom

14 August 2023

Dear Duncan

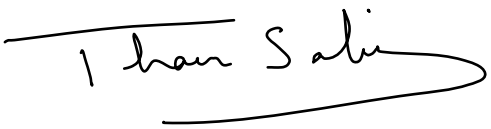
Re: EMA response to TI's report 'Together in Electric Dreams' report of March 2022

The EMA is the European 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, mobile payment instruments and cryptoasset service providers. A list of current EMA members is available on our website: https://e-ma.org/our-members.

The EMA holds Transparency International in high regard, and its members regularly rely on its reports on jurisdictions and sectors to inform its day to day risk analysis. We welcome TI's review of the electronic money sector in the UK.

Upon reviewing the report however, we have found that substantive parts of the analysis are inaccurate, impacting the main conclusions of the report. We have set these out below and we urge TI to consider our response.

Yours sincerely,



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

EMA response

1. The report's key findings

Finding (1): "Nearly 1 in 3", "Almost one-third (19,293) reports to UK law enforcement in 2019/20 relating to suspected criminal funds came from the electronic payment sector, which includes EMIs."

This is repeated at paragraph 3 of the Executive Summary which states: "In 2019/20 almost one-third (19,293) of suspicious activity reports relating to suspected criminal funds came from the electronic payment sector, of which EMIs make up a significant proportion."

This is elaborated at paragraphs 5 and 6 of the section on 'Evidence of abuse' on page 9, which provides further detail.

Response:

(i) The data and discussion under the 'evidence of abuse' section is contradictory to that in the executive summary. The 'evidence' section correctly states the e-payments sector generated 6.6%[1] of all suspicious activity reports in the UK in 2019/20. This is NOT a third of all reports to law enforcement as stated in the key facts and the summary. The statement in both the 'key findings' and Executive Summary is therefore incorrect.

(ii) This statement is made prominently in the report, in these two sections, and will be the take-away for the casual reader. Indeed the executive summary will often be the only part that is read by many, and the statement therefore has the impact of misinforming such readers.

(iii) The report further adds[2] that one third of all 'defence against money laundering' ("**DAML**") SARs were submitted by the e-payments sector -(19,293 out of a total of 62,408 for all regulated sectors). For clarity, DAMLs are reports of suspicion that are made to the NCA ahead of the processing of a transaction, that require the freezing of a customer's account or transaction, and comprise a request for guidance from the NCA on how to proceed with that transaction. They represent successful detection ahead of the completion of a transaction.

(iv) In other words, whilst the e-money sector provides 6.7% of all SARs made by the regulated sector, it is simultaneously responsible for identifying and seeking guidance on some 31% of all DAML requests from the regulated sector[3]. This would appear to be a positive statistic, where the e-payments sector is disproportionately responsible for identify and seeking guidance on suspicious

[1] Total number of SARs was 573,085, of which 38,189 related to the e-payments sector, giving a percentage of 6.7%
[2] Paragraph 6, section 'Evidence of abuse', page 9 of the report.
[3] Total number of DAMLs is 62,408, whilst e-payment submissions were 19,293, some 31% of the total.

activities BEFORE they take place, whilst generating a small part of overall SARs.

(v) As a proportion of all SARs submitted (ex post SARs and DAML), the e-money sector freezes transactions in relation to 34% of suspicions, whilst the remaining regulated sector only did so in only 8% of instances of suspicion[4]. This is a factor x4 greater rate of identification prior to the event, and of suspending transactions prior to their processing.

(vi) It is therefore inaccurate to suggest that either the e-payments sector is responsible or a third of all SARs, or to suggest that their systems and controls for combatting financial crime are inferior to those of other sectors. In fact the data demonstrates that the e-payments sector **is more effective** than other sectors.

(vii) The e-payments sector is certainly engaged in an ongoing fight against financial crime. There is however no evidence from the above facts that this sector is failing in its obligations to deter and detect such threats. The evidence is to the contrary. This may be a consequence of the more technologically up to date systems that e-payment providers deploy and which enable more effective monitoring and prevention.

Finding 2: "More than one in three (100) UK registered EMIs had money laundering red flags relating to their owners, directors or activities."

Response

(i) The fit and proper requirements for Directors and for owners (controllers) applied by the FCA are comparable to those for the entire financial services sector. In the absence of specific information, it is impossible to respond adequately to this statement. It behoves TI to provide sufficient detail and numbers, rather than to aggregate directors with owners and with activities, complicating analysis. More specific data could enable a more objective review to be undertaken.

(ii) If there are shortcomings in the approval process, these should be addressed in detail; and this should be addressed to the FCA so that it is able to remedy any oversight.

(iii) Money laundering in the UK arises from the proceeds of any crime, and this includes fraud perpetrated on the business itself on its customers and on third

[4] For e-payments the total DAMLs are 19,293, and total SARs 38,189, giving a total of 57,482; with 19,293 then making up 34% of this total. For the remainder of the regulated sector, the total number of DAMLs is 43,115, and the total number of SARs is (573,085 total – 38189 e-payments) = 534,896. This gives a percentage of those identified prior to processing as 8%.

parties. As the SAR data demonstrates, EMIs are cognoscente of their obligations in relation to preventing, detecting, and reporting on such incidents. Incidents will inevitably occur however and it is the culture, resources and know-how that are deployed that distinguish one service provider from another. The only industry-wide data available, that of SARs made, suggests good practices are in place.

Finding 3: "Using open source analysis, we found EMI licenses and accounts for sale to buyers around the world…including UK EMIs marketing their services specifically to 'high risk' customers and companies with complex ownership structures"

Response

(i) The provision of payment services to high risk sectors forms a small part of any payments activity, and whilst this raises questions over how this risk is addressed, it does not in itself give rise to a criminal endeavour. Similarly, the sale of a business, may be part of a criminal activity or may also be a legitimate sale by the owners; it is not reasonable to imply that the mere offer for sale of a business is an indicator of crime or a heightened risk.

(ii) Once an interested party proceeds in seeking to purchase an EMI, they will be subject to the same tests for fitness and propriety as the original applicant owners. The purchase of an authorised firm does not offer a shortcut or a means to avoid the fit and proper test.

(iii) We note the three example owners highlighted in the report as meriting review by the regulator, and welcome any information that identifies shortcomings in the current regime.

2. Other issues raised

(i) Abuse by criminals

The report highlights evidence of criminals targeting UK EMIs and some being utilised in the perpetration of fraud. Attempted abuse by criminals is a threat that payments industry participants have to deal with, and routinely deter and prevent. There will inevitably be instances where some crimes are committed, before they can be discovered and stopped. Internal controls and systems identify and address such risks.

It should be noted that most e-money products are intended to address a specific business sector or product proposition, rather than to offer a general purpose payment product. This creates a very clear baseline against which attempts to abuse the system can be identified. If for example, the product is targeted at students in given locations, and most transactions relate to student purchases in and around a university campus, then payments outside this area will stand out. If alternatively, a product is intended to make payments at holiday

destinations, and the payments are observed to be at unusual locations, or for unusual amounts, then again this will stand out. There are very few instances where an EMI can simply be subverted for criminal purposes without this being visible through its monitoring systems. There is good evidence that firms are identifying such discrepancies and making the requisite reports as demonstrated by the SAR figures quoted above.

(ii) Ownership and management by bad actors

This is the other main issue raised by the report, of ownership or control of EMIs by criminals. This does give rise to significant concern to industry as a whole. We are unable from the limited information set out in the report to identify the extent of any such abuse. We encourage TI to engage with the FCA on any such suspected instances to ensure that access to financial institutions in the UK by criminals in curtailed.

We do however caution against regarding all business relationships with banks or other businesses from a given geographical region as being indicative of criminality. Whilst risk associated with geographies can be heightened, there are numerous examples of responsible service providers based in such jurisdictions and providing much needed services.

(iii) Recommendation for greater regulatory attention and a multi-sector response

As set out in section 1 of this report, the SAR data is positive, industry reports 6.7% of all SARs and a third of active requests for guidance. These do NOT circumscribe an industry that is failing in its obligations

We have not addressed all issues raised in the report, some of which merit specific attention; we have confined ourselves to those issues that we are able to comment on meaningfully. We support TI's efforts in raising awareness of risks in our sector and welcome the objectives of the report.

Conclusions

- The key findings and executive summary misrepresent the proportion of suspicious activity reports made by the e-payments industry. The e-payments industry (of which EMIs are a part) are responsible for some 6.7% of all SARs, and not a third of all SARs.

- The sector is in turn responsible for a third of requests for consent SARs, which represent the identification of suspicion prior to the execution of transactions and the seeking of guidance. This is a positive statistic, much higher as a proportion of all SARs made, than other sectors.

- Other data relating to ownership or management by parties who would not meet the fit and proper test are concerning and we encourage engagement with the regulator in this regard.

- The targeting of the sector by criminals is part of the threat faced by the payments industry as a whole, and SAR data suggests that industry is implementing good practices and controls.

- Industry welcomes TI's work and any light that it shines on those parts of the industry that merit attention. We hope that our response will contribute to this and any future work.