**Electronic Money Association**
68 Square Marie-Louise
Brussels 1000
Belgium
www.e-ma.org

José Manual Campa
Chairman
European Banking Authority
EUROPLAZA
20 Avenue André Prothin
92927 Paris La Défense
France

19 April 2022

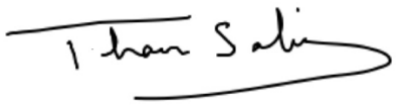
Dear José,

**Re: EMA response to EBA's preliminary observations on selected payment fraud data under PSD2, as reported by the industry**

The Electronic Money Association 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

**EMA responses**

**General remarks**

While the EMA welcomes these observations on selected payment fraud data under PSD2, this data would be more useful for the industry if it were more detailed, and perhaps with additional input from law enforcement and Financial Intelligence Units (FIUs) for example.

A higher level of granularity would better serve the objective of the PSD2 fraud data collection, as it would allow firms to better understand and assess the ever-changing fraud trends in the payment sector, and increase the effectiveness of their fraud prevention tools. Reporting fraud data to NCAs has become an increasingly burdensome activity for PSPs, so without such granularity it will become a fruitless exercise. On the other hand, being able to use aggregated data that is sufficiently detailed to allow firms to improve their own anti-fraud tools and processes would meet one of key the objectives of the data collection exercise; the prevention of fraud.

**Question 1**: ***Do you have any views on the high share of cross-border frauds in the total volume of fraud?***

No comment

**Question 2**: ***Do you have any comments on the patterns that are outlined in the chapter "patterns emerging from the selected data"?***

Regarding the occurrence of different types of fraud, for non-remote card payments, lost or stolen cards represent 45 % of the value of the fraudulent payments authenticated with SCA. For remote card payments, lost or stolen cards also represent 75 % of the value of the fraudulent SCA payments. This is likely because until 31 December 2020, mere possession of a payment card would be adequate to carry out fraudulent transaction; there was no need for the fraudster to offer a 2nd authentication element and on-card data were accepted as a cardholder authentication credential. For data reported after 31 December 2020, when SCA was introduced for remote card transactions, it is to be expected that this value will decrease, as the possession of the card is no longer enough to allow the fraudster to initiate a payment transaction that will be authorised.

**Question 3**: ***Do you have any potential further explanations as to why, in the specific case of the remote credit transfers, the fraud rate reported by the industry is higher for payments authenticated with SCA compared to payments that are not authenticated with SCA?***

In line with one of the potential explanations mentioned by the EBA, the likely explanation for the divergence in observed fraud rates for Credit Transfers (CTs) is that fraudsters will use social

engineering/payer manipulation attacks to initiate Credit Transfers from the victims' accounts and successfully complete SCA using either stolen SCA credentials or by manipulating the actions of the legitimate account holder.

**Question 4**: ***Do you have any potential explanations why PSUs bear most of the losses due to fraud for credit transfers and cash withdrawals?***

No comment

**Question 5:** ***Do you have any potential explanations why the percentage of losses borne by the PSUs substantially differs across the EEA countries?***

No comment

**Question 6:** ***Do you have any potential explanations why the industry has reported fraud losses as having been borne mostly or significantly by "others"?***

A possible explanation is that the "Others" are the Retailers/Merchants involved in fraudulent payment transactions, who have absorbed the relevant financial burden. To mitigate this effect, the EBA could review the granularity of the fraud loss-bearing entity taxonomy listed in the EBA Guidelines, to align it better with the payment ecosystem entities that record financial fraud losses.

**Question 7**: ***Do you have any views regarding the observed correlation between the value of fraud and the value of losses due to fraud between H2 2019 and H2 2020?***

No comment

**Question 8**: ***How do you explain the fact that the manipulation of the payer by the fraudster represents a substantial share of the fraudulent non-remote credit transfers authenticated with SCA? How is this fraud type concretely executed by the fraudsters?***

A possible explanation is that non-remote payments is often a solution chosen by older people, who are also more likely to be a target for payer manipulation (social engineering) fraud. A second explanation is that in some cases, higher value credit transfers must be done in person, at the location of the PSP, and cannot be done remotely. Typically, this fraud type involves the fraudster convincing the account holder to execute the credit transfer (to an account controlled by the fraudster) in

person. The fraudster uses social engineering methods to establish credibility with the account holder over a period of time before "proposing" to the account holder to carry out the credit transfer in person. In any case, increased PSP staff and PSU awareness and the deployment of some type of Confirmation of Payee scheme appear to be the main security controls that the payment industry can currently bring to bear to limit the growth of this fraud type, going forward. A more holistic fraud management approach to combat payer manipulation fraud types that involves non-regulated entities (search engine providers, social media platform providers, website hosting providers etc.) may be needed to target certain payer manipulation fraud types (Investment fraud, Romance Fraud etc.)

**Question 9**: ***Do you have any views regarding the types of card payment fraud that have been reported by the industry under the category "issuance of a payment order by the fraudster", sub- category "others"?***

The EMA does not have a view regarding the types of card payment fraud that have been reported by the industry under the category "issuance of a payment order by the fraudster", sub- category "others". However, the high percentage of the "others" category may be the sign of an issue, as there is possibly a lack of clarity. It might be necessary to review the categories.

**Members of the EMA, as of April 2022**

AAVE LIMITED
Account Technologies
Airbnb Inc
Airwallex (UK) Limited
Allegro Group
American Express
ArcaPay Ltd
Azimo Limited
Banked
Bitpanda Payments GmbH
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network Ltd
Boku Inc
CashFlows
Circle
Citadel Commerce UK Ltd
Contis
Corner Banca SA
Crypto.com
Curve
eBay Sarl
ECOMMPAY Limited
Em@ney Plc
emerchantpay Group Ltd
ePayments Systems Limited
Etsy Ireland UC
Euronet Worldwide Inc
Facebook Payments International Ltd
Financial House Limited
First Rate Exchange Services
FIS
Flex-e-card
Flywire
Gemini
Global Currency Exchange Network Limited
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
NOELSE PAY
NoFrixion Ltd
OFX
OKTO
One Money Mail Ltd
OpenPayd
Own.Solutions
Oxygen
Park Card Services Limited
Paydoo Payments UAB
Paymentsense Limited
Payoneer Europe Limited
PayPal Europe Ltd
Paysafe Group
Plaid
PPRO Financial Ltd
PPS
Ramp Swaps Ltd
Remitly
Revolut
SafeCharge UK Limited
Securiclick Limited
Skrill Limited
Soldo Financial Services Ireland DAC
Square
Stripe
SumUp Limited
Syspay Ltd
Transact Payments Limited
TransferMate Global Payments
TrueLayer Limited
Trustly Group AB
Uber BV
Vitesse PSP Ltd
Viva Payments SA
Weavr Limited
WEX Europe UK Limited
Wirex Limited
Wise
WorldFirst
WorldRemit LTD
Yapily Ltd