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

Rt Hon. Mel Stride MP
Chair of the Economic Crime Enquiry,
Treasury Committee,
Houses of Parliament
Palace of Westminster
London
SW1A 0AA

27 November 2020

Dear Mr Stride,

Re: Call for evidence for the enquiry on Economic Crime

We very much welcome the opportunity to provide input to the Economic Crime Enquiry's call for evidence into Economic Crime.

The EMA is the EU trade body of FinTech and BigTech firms engaging in the provision of alternative payment services and the issuance of electronic money. Our members include leading payments and e-commerce businesses providing online/mobile payments, card-based products, electronic vouchers, virtual currency exchanges, electronic marketplaces, merchant acquiring services and a range of other innovative payment services. A list of current EMA members is provided at the end of this document.

The Treasury Committee invites written evidence as regards the UK's AML and sanctions regimes, and economic crime affecting consumers:

i. Concerns regarding or improvements to the UK's anti-money laundering and the sanctions regimes, including but not limited to:

The work of OPBAS and the profession body AML supervisors

No Comment.

The impact of the FinCEN papers

No Comment.

Corporate liability for economic crime

No Comment.

The work of Companies House

Companies House reform is long overdue and should be a priority. The agency holds a key gatekeeper function in the formation of companies, and the process must be robust enough to deter the use of UK registered companies for money laundering purposes, as has been seen in recent reports on the FINCEN data leak. Reform of Companies House processes - particularly due diligence – is desirable, as well as an increase in staff resources to manage the extra workload that would inevitably result from a more robust governance and management regime.

Under Money Laundering Regulations (MLRs)[1] firms must report any discrepancies between the information on 'beneficial owners' (MLR definition) they already hold and the information on 'persons of significant control' (PSCs) that is on the Companies House register. We welcome the many plans for reform of Companies House, the bolstering of the reliability of data that it hosts, and the updating of its systems and processes.

However, the current system for notifying discrepancies of the PSC register does not allow for any bulk reporting of discrepancies.

It is inefficient for firms to have report discrepancies on an individual basis using the companies house portal as it currently stands, particularly for firms that operate a platform, where high numbers of business customers are onboarded on a daily basis. Consideration should be given as a matter of priority to the development of a system where firms could potentially use an Application Programming Interface (API) to deliver the data related to any PSC register discrepancies.

As a final note we would like to stress the value in terms of due diligence that could be placed upon an improved and more robust Companies House register of companies. It would become an even more trusted source for information and verification purposes when corporate customers are being onboarded within the sector. It is already very well used for due diligence purposes but adding further levels of governance and rigour to the process including powers to query, seek evidence and remove information that is incorrect are a key step in enhancing AML controls at Companies House and making the use of UK Registered companies for money laundering purposes a less attractive option.

ii. Consumers and economic crime, including but not limited to:

[1] https://www.legislation.gov.uk/uksi/2017/692/contents

Any emerging trends in consumer facing economic crime as a result of the COVID crisis

The EMA has provided evidence to support the National Crime Agency annual strategic report on organised crime in relation to money laundering. Firms have witnessed the increase of certain types of Fraud during the COVID-19 pandemic due to an exponential increase in the volume and values of online transactions, and a greater use of online market places, particularly by consumers that are less tech savvy.

The use of social engineering in all fraud types is on the increase and is used by criminals to launder the proceeds of crime and also to commit fraud. The common types of underlying scams noted by EMA members are often targeted at less tech savvy victims –traditional scams where the victim is offered a fake prize or reward and then is duped to give personal details and pay a fee to receive the gift.

Another prevalent typology under COVID-19 is the sale of goods online not being supplied or delivered after payment. Again, given the increase in online transactions, an increase in this type of scam is inevitable.

The most effective tool to reduce the prevalence of these frauds is a greater focus on warning consumers of such scams through education and targeted awareness campaigns in the online market places where victims are often duped. Fraud reduction measures should also include potential blocking of fraudulent adverts and greater cooperation with social media operators to reduce their use for fraudulent purposes. In this area the social media companies and online market places have a key role to play and should be encouraged to participate through government intervention.

The operation of the Contingent Reimbursement Model for Authorised Push Payment Fraud

The EMA has followed the development of the Contingent Reimbursement Model for Authorised Push Payment Fraud from inception, and broadly supports the goals of the Code, as well as welcoming the impact so far.

However, we understand there are several demands for the mandatory adoption of the Code for all regulated Payment Service Providers, either through legislation or through a Faster Payments Scheme (FPS) rule change. The EMA does not support either approach, but instead we propose a number of alternative solutions that are more likely to be effective in reducing the incidence of APP scams.

The EMA does not support the compulsory adoption of the Code across the payments industry at this stage – at least not in its current form. The current version of the Code is not well suited for certain PSPs and in particular smaller non-banks, who have significantly smaller customer service and complaint handling teams than UK banks, and who experience far lower levels of APP fraud. It is also not clear that a mandatory adoption of the Code in its current form would improve the outcome for customers across the UK, or even reduce the frequency, volume or value of APP scams.

The EMA has a diverse membership across the payments sector who adopt a number of different business models. Mandatory adoption of the CRM Code would place a disproportionate financial burden on firms who for example primarily focus on cross-border payments, but for whom a very limited number of users are affected by domestic APP scams. Pursuing the blanket application of this Code for all businesses in the UK, without regard to risk and business model, would create a barrier to entry for firms with non-banks or non-traditional models. This is likely to stifle innovation and competition in the market.

Brexit has already placed a significant financial and resource drain on many EMA members, with most firms having to set up mirror operations in other EU jurisdictions in order to continue to provide services to their existing EU customer base. Increasing the administrative burden for those that remain in the UK, particularly those with a cross border focus, may act as a tipping point to their exit from the UK market.

The CRM code can be enhanced through continued investment in technological terms to prevent APP scams - but is not fit for purpose for compulsory usage in its current form. Instead there is scope for private sector innovation to offer consumer protection against purchase scams through the development and use of overlay services. Applying legislative measures will have many unintended consequences on the UK payments market.

The Faster Payments Scheme (FPS) has a service level agreement in place, which requires a minimum percentage of faster payments to be 'real-time'. This supports and could encourage the uptake of FPS as a payment method at point of sale (POS) as well as online (e-commerce). Particularly with the growth in the Payment Initiation Service (PIS) sector, FPS now offers a viable alternative to cards, the latter of which still lay claim to the highest fraud losses by value[2]. However, such innovative solutions may lose their attractiveness if FPS is no longer guaranteed to settle instantly, for example with the introduction of an FPS rule change the introduces a delay in the execution of payments.

FPS service level agreements allow personal financial management transactions to be made with minimal friction. The introduction of additional friction will make it harder for individuals to take advantage of these payment services, which are largely legitimate and pose little risk. In conclusion, FPS is used for many different use cases and payment reasons which have varying degrees of fraud risk. A blanket scheme change that adds friction to all transactions regardless of risk is not efficient, proportionate or fair.

Instead, the Code should be supported by a framework that better enables firms to safely freeze and repatriate the funds out of the hands of scammers. Currently, the legal framework does not empower firms to effectively support consumers who wish to attempt to prosecute the individual who scammed them. Further steps to disincentivise fraudsters using these scams needs to be rolled out. Possible solutions could include:

- removing fraudsters from online marketplaces
- working with telecoms and social media companies to prevent fraudulent ads
- further investment in preventative technological options to scams

[2] UK Finance Fraud the Facts 2020: https://www.ukfinance.org.uk/system/files/Fraud-The-Facts-2020-FINAL-ONLINE-11-June.pdf

The response of financial institutions to economic crime as it affects consumers

No Comment.

Yours sincerely,

Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

List of EMA members as of November 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
Financial House Limited
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 Limited
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