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

HM Treasury
Anti-MoneyLaunderingBranch@hmtreasury.gov.uk

June 2019

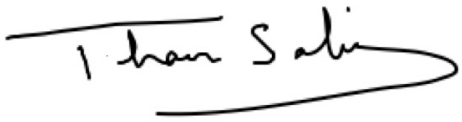
Dear Sir/Madam,

Re: EMA response to 5MLD transposition consultation

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, mobile payment instruments and virtual currency-related services. 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.

We welcome the opportunity to provide a response to HMT's consultation on the transposition of the 5th Money Laundering Directive in the UK. In what follows below we set out our views and provide evidence in response to the questions relevant to the EMA's membership. We would be grateful for your consideration of our response and are available should you have any questions.

Yours sincerely,



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

PIS/AIS Providers

EMA Response

We note that no reference has been made in this consultation to the recent inclusion of Payment Initiation and Account Information Service Providers amongst the list of financial institutions as obliged entities. It would be helpful to industry to clarify whether both of these types of institution will indeed be regulated, and the applicability of different parts of the AML regime.

This clarification could address Account Information Service Providers in particular, as they are not involved in the execution of any transactions. Additionally, although Account Information Service Providers are captured by the definition of financial institution, the European Commission has indicated informally that they did not intend to include them within the scope. Consequently, a number of European member states chose not to regulate Account Information Service Providers. This is consistent with the prohibition for these institutions from requesting sensitive payment data (Article 67(2)(e) 2PSD), which may impact their ability to conduct CDD and file SARs.

In relation to Payment Initiation Service Providers, it would be helpful to clarify which parts of the MLR apply to their services. Payment Initiation Service Providers currently deliver their service to, and contract with, the merchant, rather than the payer consumer. Therefore, there should be no obligation to conduct CDD on payer consumers. The prohibition for these institutions to store sensitive payment data (Article 66(3)(e) 2PSD) may, however, impact their ability to conduct CDD even on merchants, and may hinder the filing of SARs. It will be vital to define the meaning of sensitive payment data in this context and how obligations under the PSR should be reconciled with those under AML legislation.

Box 2.C: Cryptoassets

Question 12 *5MLD defines virtual currencies as "a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically". The Government considers that all relevant activity involving exchange, security and utility tokens should be captured for the purposes of AML/CTF regulation, and seeks views on this approach. Is the 5MLD*

definition appropriate or does it need to be amended in order to capture these three types of cryptoassets (as set out in the Cryptoassets Taskforce's framework)? Further, are there assets likely to be considered a virtual currency or cryptoasset which falls within the 5MLD definition, but not within the Taskforce's framework?

EMA Response

The terms 'currency' and 'means of exchange' in the 5MLD definition suggest that only exchange or payment tokens are captured. In order to capture exchange, security and utility tokens, the following amended FATF definition of 'virtual asset' should be adopted instead: 'A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already regulated.' Such a comprehensive definition will allow for uniform application of AML regulation across the broad cryptocurrency sector.

It should also be clarified how the boundary between utility tokens with a substantive AML risk and traditional loyalty/incentive products as well as in-game currencies that can only be used within a specific environment (see Recital 7(a) 5MLD) will be drawn. In this respect, it is not clear how secondary trading of these tokens would affect their regulated status (and consequently, the status of the trading exchange). We also welcome the fact that the Taskforce's definition makes it clear that any assets which act as cryptoassets but are not cryptographically secure are not covered.

Question 13 *5MLD defines a custodian wallet provider as "an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies". The Government considers that all relevant activity involving exchange, security and utility tokens should be captured for the purposes of AML/CTF regulation, and seeks views on this approach. Is the 5MLD definition appropriate or does it need to be amended in order to capture these three types of cryptoassets (as set out in the Cryptoassets Taskforce's framework)? Further, are there wallet services or service providers likely to be considered as such which fall outside the 5MLD definition, but should come within the UK's regime?*

EMA Response

The definition should emphasize that the term 'custodian wallet provider' applies only to those providers who have control over users' virtual currency. Control in this context

means the 'power to execute unilaterally or prevent indefinitely a virtual currency transaction' (Uniform Regulation of Virtual Currency Businesses Act). Providers of wallets without control over the virtual currency, where users either manage their own keys, such keys are held outside of the wallets in a third party provider's ecosystem or where multiple signatures are required in order to effect transactions should not fall within the definition (these are 'non-custodian wallet providers'). Such providers are simply providing IT services to users, in the same way as cloud hosting service providers provide services to users.

We do not envisage that there are any wallet services or service providers likely to be considered as falling outside the 5MLD definition but that should come within the UK's regime.

Question 14 *Should the FCA be assigned the role of supervisor of cryptoasset exchanges and custodian wallet providers? If not, then which organisation should be assigned this role?*

EMA Response

To regulate a sector as diverse as that of cryptoassets requires knowledge of different financial instruments, particularly if ICOs are also included in the scope of regulation. We believe that the FCA has the requisite experience and knowledge and is therefore best suited for this role. In fact, the FCA is already supervising some authorized financial services firms providing services (which are currently unregulated) in relation to cryptoassets.

Question 15 *The government would welcome views on the scale and extent of illicit activity risks around cryptoassets. Are there any additional sources of risks, or types of illicit activity, that this consultation has not identified?*

EMA Response

We believe that the Taskforce's review sufficiently identifies the current key areas of risk.

Question 16 *The government would welcome views on whether cryptoasset ATMs should be required to fulfil AML/CTF obligations on their customers, as set out in the regulations. If so, at what point should they be required to do this? For example, before an 'occasional transaction' is carried out? Should there be a value threshold for conducting CDD checks? If so, what should this threshold be?*

EMA Response

Overall, we welcome a harmonised approach to regulation of cryptoassets at European and, ideally, global level. Gold-plating, i.e. the introduction of additional obligations at national level, may eventually lead to competitive disadvantages for UK firms and should be avoided unless there is a compelling reason to take a different approach. At first glance, it is sensible that cryptoasset ATMs should be required to perform some level of CDD, given that they are fiat on/off ramps and operate like an exchange. The situation should be avoided whereby an ATM has only a 'per session' fiat limit, which could be circumvented through repeated transactions to different wallets. On a practical level, this may, however, be difficult to implement.

Question 17 *The government would welcome views on whether firms offering exchange services between cryptoassets (including value transactions, such as Bitcoin-to-Bitcoin exchange), in addition to those offering exchange services between cryptoassets and fiat currencies, should be required to fulfil AML/CTF obligations on their customers.*

EMA Response

As gatekeepers to the regulated financial system, crypto-to-fiat exchanges are the appropriate starting point for the regulation of the cryptoassets sector. This is also consistent with a line-by-line transposition of 5MLD, which we welcome (see Q16 above). As cryptoassets become more prominent and the retail take-up of these assets increases, crypto-to-crypto exchanges may also warrant regulation. This should, however, be evidence-based, and not preemptive.

Question 18 *The government would welcome views on whether firms facilitating peer-to-peer exchange services should be required to fulfil AML/CTF obligations on their users, as set out in the regulations. If so, which kinds of peer-to-peer exchange services should be required to do so?*

EMA Response

There are a number of different types of P2P exchanges, and these may only be distinguishable on a case-by-case basis. For example, some exchanges have liquidity pools, some only match parties, with settlement happening off the exchange. Others again only allow for advertising of a sale, with no software-enabled match taking place. It is often difficult to determine whether there is an administrative or custodial function. The regulation of P2P exchanges should therefore be postponed until business practices mature, and specific risks are identified.

Question 19 *The government would welcome views on whether the publication of open-source software should be subject to CDD requirements. If so, under which circumstances should these activities be subject to these requirements? If so, in what circumstances should the legislation deem software users be deemed a customer, or to be entering into a business relationship, with the publisher?*

EMA Response

The publication of software does not involve an innate risk of money laundering, and publication does not therefore merit inclusion within the scope of obliged persons. Similarly, users of software per se cannot be regarded as engaging in a regulated activity that qualifies a 'a business relationship' under AML legislation and must therefore trigger CDD obligations. In fact, such an approach would go against expression rights. A more specific approach must be developed that identifies classes of activity that merit inclusion within the scope of obliged persons and activities. Publication of software does not appear to qualify as such an activity. Adopting such an approach would almost certainly put the UK at a competitive disadvantage in the global technology space.

Question 20 *The government would welcome views on whether firms involved in the issuance of new cryptoassets through Initial Coin Offerings or other distribution mechanisms should be required to fulfil AML/CTF obligations on their customers (i.e. token purchasers), as set out in the regulations.*

EMA Response

ICOs have been used to raise funds for various types of investment and also as a proxy for other financial instruments. They have also been associated with fraudulent investment proposals. It would be appropriate to apply AML obligations in circumstances where equivalent non-crypto services were subject to AML obligations. Where the activity is novel and is not analogous to a non-crypto activity however, then it will need to be considered on its merits.

Question 21 *How much would it cost for cryptoasset service providers to implement these requirements (including carrying out CDD checks, training costs for staff, and risk assessment costs)? Would this differ for different sorts of providers?*

EMA Response

Most cryptoasset providers regard the development and application of AML controls as a necessary part of a regulatory framework. They will, however, seek to implement a risk-based approach to use resources in the most effective manner.

As in most cases, the cost will differ depending on the size of the firm, jurisdiction of the customer and whether the firm has a predominately retail or institutional customer base. In the case of a retail-heavy customer base, the cost will likely range between £2 - £20 to complete full ID & verification. The cost would substantially increase for a predominately institutional customer base.

Question 22 *To what extent are firms expected to be covered by the regulations already conducting due diligence in line with the new requirements that will apply to them? Where applicable, how are firms conducting these due diligence checks, ongoing monitoring processes, and conducting suspicious activity reporting?*

EMA Response

Most UK-based fiat-to-crypto exchanges have implemented CDD procedures already, perhaps in anticipation of regulation. This does not appear to be as common for crypto-to-crypto exchanges. Additionally, some firms are adopting CDD procedures that comply with e-money and payment services regulation. It appears that many of the established exchanges in the UK have a SAR reporting process in place.

Question 23 *How many firms providing cryptoasset exchange or custody services are based in the UK? How many firms provide a combination of some of these services?*

EMA Response

The EMA is not aware of the total number of UK-based firms providing cryptoasset exchange or custody services or a combination of some of these services.

24 *The global, borderless nature of cryptoassets (and the associated services outlined above) raise various cross-border concerns regarding their illicit abuse, including around regulatory arbitrage itself. How concerned should the government be about these risks, and how could the government effectively address these risks?*

EMA Comments

We believe that the imminent FATF Guidelines will mitigate this risk.

If regulation were to be extended to foreign firms offering their products to UK consumers, most providers would simply not offer their products in the UK. This would result in UK consumers being denied access to these products, with UK user benefits being eroded. A compromise proposal that would also address regulatory arbitrage could see a restriction implemented by which only products from those countries are blocked that do not have an equivalent regulatory regime in place (which is the approach taken by Japan). In that case, multi-national exchanges with UK operations should be required to prove that they are not commingling funds across their entities. It should, however, be borne in mind that for providers to establish where a token comes from and whether it comes from an off-jurisdiction exchange is expensive and time consuming, as it involves extensive data collection and analysis.

Question 25 *What approach, if any, should the government take to addressing the risks posed by "privacy coins"? What is the scale and extent of the risks posed by privacy coins? Are they a high-risk factor in all cases? How should CDD obligations apply when a privacy coin is involved?*

EMA Comments

At present, the term "privacy coin" is ambiguous. We would request that this term is properly defined in the first instance. In any event, it appears that what are colloquially deemed to be privacy coins are becoming easier to trace and, as a market response, new coins are thus being developed in order to ensure continued anonymity.

Box 3.A: Electronic money

Question 37 *Should the government apply the CDD exemptions in 5MLD for electronic money (e-money)?*

EMA Response

Yes. The CDD exemptions for e-money are an important means of enabling the take-up of low-risk products without an undue burden on consumers to undergo verification of identity procedures. The CDD exemptions were initially introduced to allow easy access to low-value, low-risk e-money products. Consumers often use these types of products for small online spends that guarantee a high-level of security and privacy and that allows the customers to be in full control of their costs.

While in their current, highly restricted form the exemptions are of value to a narrow range of e-money products, several of our members use and intend to continue utilise them for their products in the manner provided for in the MLRs.

Question 38 *Should e-money products which do not meet the criteria for the CDD exemptions in Article 12 4MLD as amended be considered for SDD under Article 15?*

EMA Response

Yes. Reg. 38(4) of the MLR 2017 set out that issuers who do not meet the criteria in Article 12 may nevertheless apply SDD under Article 15, and this provision should be put in place. Article 15 SDD is predicated on a risk assessment and a documented finding of low risk before it can be adopted. It therefore offers flexibility based on the risk and the mitigation strategy adopted to address ML/TF. It also requires a response to the various elements of CDD (initial, ongoing, monitoring etc) rather than an exemption from the requirement to apply any part of the CDD regime, and is therefore an appropriate component of the AML regime for e-money products.

Question 39 *Should the government exclude any e-money products from both the CDD exemptions in Article 12, and from eligibility for SDD in Article 15?*

EMA Response

No. We believe that general/blanket exclusions would wholly contradict the principle of a risk-based approach enshrined in both 4MLD and 5MLD. All e-money products that either meet the criteria in Article 12 or can evidence the low risk required for the application of SDD in Article 15 should be able to take advantage of these provisions.

Question 40 *Please provide credible, cogent and open-source evidence of the risk posed by electronic money products, the efficacy of current monitoring systems to deal with risk and any other evidence demonstrating either high or low risk.*

EMA Response

For an open-source account of risk, please see the EBA risk factor guidelines and the sectoral guidance on e-money contained in Part II of the JMLSG guidance notes.

Question 41 *What kind of changes, if any, will financial institutions and credit institutions have to implement in order to detect whether anonymous card issuers located in non-EU equivalent states are subject to requirements in their national legislation which have an equivalent effect to the MLRs?*

EMA Response

This requirement brought in by 5MLD is onerous and will need to be implemented by card schemes as part of their rules. Whilst we support the goal of the new paragraph 12(3), we have serious concerns regarding the practical feasibility of implementing the requirements. It will be difficult for individual acquirers to implement their own rules as to which cards will be accepted in payment based on the country of origin. Knowledge of the different CDD requirements in different countries is a demanding requirement and is unlikely to be fulfilled by most acquirers without assistance from card schemes or some other third party. Furthermore, this will need to be assessed on an ongoing basis. At the time of the negotiation of the Directive, the card schemes indicated a willingness to implement appropriate controls, and this was the basis upon which the provision was accepted.

Question 42 *Should the government allow payments to be carried out in the UK using anonymous prepaid cards? If not, how should anonymous prepaid cards be defined?*

EMA Response

As the use of cash diminishes, the ability of individuals to make payments of limited amounts privately is eroded. It is not an unreasonable expectation for users to be able to undertake transactions in a private manner, to allow for personal preference, political choices and a quest for privacy to be fulfilled. A prohibition on anonymous payments would also have far-reaching consequences for vulnerable consumer groups – such as the financially excluded – who, in many cases, rely on these types of cards.

An informative quote from a different era reads as follows:

"In a sense, a person is defined by the cheques he writes, By examining them, the agents get to know his doctors, lawyers, creditors, political allies, social connections, religious affiliations, educational interests, the papers and magazines he reads and so on ad infinitum"

This is a quote from Douglas J in the US Supreme Court in the case of the California Bankers Association v Shultz US 21 (1975).

Records of transactions have the potential to erode privacy entirely, and with the ability to monitor transactions in real time, the impact is the more acute.

Box 10.A: National register of bank account ownership

82 *Do you agree with, or have any comments upon, the envisaged minimum scope of application of the national register of bank account ownership?*

EMA Response

In principle we do not object to the inclusion of payment accounts identified by an IBAN on the register. However, single and short-term-use payment products do not merit inclusion in the scope of the register even when they are identified by an IBAN, as the cost to business outweighs the benefits to law enforcement. An example of a single-use product is a one-time virtual card used by a corporate to pay expenses. An example of a short-term-use product is a non-reloadable prepaid card. For both these types of product, law enforcement agencies can continue to seek information from trade bodies such as the EMA and from individual regulated entities.

Question 83 *Can you provide any evidence of the benefits to law enforcement authorities, or of the additional costs to firms, that would follow from credit cards and/or prepaid cards issued by e-money firms; and/or accounts issued by credit unions and building societies that are not identifiable by IBAN, being in scope of the national register of bank account ownership?*

EMA Response

We oppose the inclusion of prepaid cards not identified by an IBAN in the scope of the register. The functionality of products without an IBAN is restricted and does not meet the rationale for the introduction of the register by the Directive. The inclusion of such products was extensively discussed at the time the directive was negotiated, when it was thought that the condition of identification by IBAN would ensure a balance between the costs of inclusion on regulated entities and the associated benefits to law enforcement. For these types of product, law enforcement agencies can continue to seek information through trade bodies and from individual regulated entities about their ownership. Please also refer to our response to question 84 below.

Question 84 *Do you agree with, or have any comments upon, the envisaged scope of information to be included on the national register of bank account ownership, across different categories of account/product?*

EMA Response

We suggest that the minimum requirements set out at Article 32(a)(3) of 5MLD be adhered to; and any additional information can then be sought from the relevant account holding financial institution. This should minimise the administrative burden on PSPs, it would lessen the impact of a successful intrusive attack on the register, and minimise the need for continuously updating the register.

Question 85 *Do you agree with, or have any comments upon, the envisaged approach to access to information included on the national register of bank account ownership?*

EMA Response

The information that will be included on the register will have significant fraud value. It is therefore of utmost importance that the register is as secure as reasonably possible, and government should set out the steps it will take to ensure the security of the register. If the register were to be successfully accessed by intruders, every financial institution (as well as many non-financial institutions, such as utility providers) would likely need to amend the security questions they rely upon when authenticating their customers. Such an attack would therefore come at a great cost to industry and society.

Question 87 *Do you agree with, or have any comments upon, the envisaged frequency with which firms will be required to update information contained on the register? Do you have any comments on the advantages/disadvantages of the register being established via a 'submission' mechanism, rather than as a 'retrieval' mechanism?*

EMA Response

The suggestion to establish a retrieval mechanism through APIs is resisted. End users of APIs want to have certainty that third parties can only access their information with their permission, and they want to have control over what information third parties will be able to access. Giving access to financial information to government agencies through APIs is likely to result in an erosion of trust in these services.

Box 14.G: New technologies

Question 104 *Should regulation 19(4)(c) be amended to explicitly require financial institutions to undertake risk assessments prior to the launch or use of new products, new business practices and delivery mechanisms? Would this change impose any additional burdens?*

EMA Response

We note the reference to Criterion 15.2 in the FATF Mutual Evaluation Report of the UK of 2018.

Most regulated entities within the e-money and payments sector already undertake risk assessments prior to the launch or use of new products, new business practices and delivery mechanisms in accordance with JMLSG guidance. The introduction of a new legally-binding requirement in this respect would therefore have limited impact on existing industry practice.

Box 14.H: Group policies

Question 105 *Should regulation 20(1)(b) be amended to specifically require relevant persons to have policies relating to the provision of customer, account and transaction information from branches and subsidiaries of financial groups? What additional benefits or costs would this entail?*

EMA Response

We note the reference to Criterion 18.2(b) in the FATF Mutual Evaluation Report of the UK of 2018.

It is unclear what purpose the FATF sees in the provision of customer, account and transaction information from branches and subsidiaries of financial groups to the parent undertaking if not for the purposes of AML/CTF risk assessment (which is the subject of Criterion 18.2(a)) or SAR reporting (which is excluded by the last sentence in Criterion 18(2)(b)). Reg. 20(1)(b) MLR 2017 already provides for controls and procedures where information is shared within the group for AML/CTF purposes. Before imposing a new requirement to actively share information, it should be established what purpose this information sharing should serve.

List of EMA members as of June 2019

AAVE LIMITED
Airbnb Inc
Airwallex (UK) Limited
Allegro Group
American Express
Azimo Limited
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network Ltd
Boku Inc
CashFlows
Circle
Citadel Commerce UK Ltd
Coinbase
Corner Banca SA
Curve
eBay Sarl
ePayments Systems Limited
Euronet Worldwide Inc
Facebook Payments International Ltd
First Rate Exchange Services
Flex-e-card
Flywire
GoCardless Ltd
Google Payment Ltd
IDT Financial Services Limited
Imagor SA
Intuit Inc.
Ixaris Systems Ltd
Moneyhub Financial Technology Ltd
MuchBetter
myPOS Europe Limited
Nvayo Limited
One Money Mail Ltd
OpenPayd
Optal
Park Card Services Limited
Paybase Limited
Paydoo Payments UAB
Payoneer
PayPal Europe Ltd
Paysafe Group
PPRO Financial Ltd
PrePay Solutions
QIX Ltd
Remitly
Revolut
SafeCharge UK Limited
Securiclick Limited
Skrill Limited
Stripe
SumUp Limited
Syspay Ltd
Transact Payments Limited
Transact24 (UK) Ltd
TransferMate Global Payments
TransferWise Ltd
TrueLayer Limited
Trustly Group AB
Uber BV
Valitor
Vitesse PSP Ltd
Viva Payments SA
Wirecard AG
Wirex Limited
WorldFirst
Worldpay UK Limited