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

Sanctions and Illicit Finance Team (2nd Floor)
HM Treasury
1 Horse Guards Road
London SW1A 2HQ
Anti-MoneyLaunderingBranch@hmtreasury.gov.uk

18 June 2024

Dear Madam/Sir,

Re: EMA response to HM Treasury's consultation on improving the effectiveness of the Money Laundering Regulations

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 services. A list of current EMA members is available on our website: https://e-ma.org/our-members.

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

Customer Due Diligence

Due diligence triggers for non-financial firms

Q1: Are the customer due diligence triggers in regulation 27 sufficiently clear?

EMA response:

1. In relation to CASPs:
    a. It is unclear how the EUR 1,000 threshold for cryptoasset transfers in regulation 27(7E) can be combined with regulation 64C(8), which requires verification of the information obtained in accordance with regulation 64C(1) without the application of any threshold.
    b. It would also be helpful for CASPs (as well as for other obliged entities) to have more clarity on the kinds of customer interactions that might lead to a business relationship or occasional transaction, i.e., that are in scope of the MLRs. For instance, a customer may have a relationship with a CASP for an unregulated service, such as the use of their software. Would this relationship need to be taken into account when determining whether there is a business relationship for the purposes of the MLRs?
2. More generally, we think that the current triggers for CDD can, and should, be made significantly more effective, as it is not always clear when a business relationship arises.
    a. Business relationship trigger: The trigger of when a business relationship is established should allow firms to take the view that a business relationship only arises when a customer first undertakes a transaction, i.e., when the economic activity commences, not simply when a customer agrees to a firm's terms and conditions. This would better reflect the reality of the start of the relationship and would be proportionate and risk-based. It would place the impact of CDD requirements on the customer experience at the most pertinent time, i.e., when the customer wants to undertake a transaction, not simply when they have entered a contractual relationship.
    b. Furthermore, once the customer has commenced transactions, it is not always clear when these amount to a business relationship. Customers may, for example, transact sporadically, with long intervals between transactions. It would be helpful for firms to be able to set reasonable parameters for a business relationship to arise, such as a minimum number of transactions that needs to have been undertaken or a certain amount of time during which the relationship persists.
    c. Occasional transaction (€1,000) trigger: In practice, this trigger can only rarely be relied upon, because the business relationship trigger trumps it. To be effective, such a *de minimis* threshold needs to be woven into the business relationship trigger, so that a firm may choose (based on a risk-based approach) whether to apply CDD measures upon entry into contractual arrangements (i.e., acceptance of terms and conditions) with a customer, a customer's first transaction, or a customer's transaction or series of related transactions reaching the *de minimis* monetary threshold (€1,000).

Verifying whether someone is acting on behalf of a customer

Q3: Do you think the wording in regulation 28(10) on necessary due diligence on persons acting on behalf of a customer is sufficiently clear? If not, what could help provide further clarity?

EMA response:

1. The requirement around due diligence on persons 'acting on behalf of' a customer must be made clearer. First, with respect to corporate customers, there should be no mandatory requirement to verify that persons have the authority to act on behalf of the customer and to identify and verify the identity of such persons. Employees of the corporate customer are (understandably) often reticent to provide personal data for these purposes when the business relationship or transaction is solely for the benefit of the corporate. Additionally, this should be a risk-based decision for a firm taking account of a person's title, or role, and the firm's overall assessment of the risk relevant to the corporate customer. Second, in relation to individuals, while there may be some occasions where a formal appointment is made (e.g., an executor of a will), again a firm should be able to take a risk-based approach both as to the degree of evidence of the person's authority to act on behalf of the customer and the degree of verification of their identity required in the circumstances.

Enhanced Due Diligence

General triggers for enhanced due diligence

Q11: Are there any other risk factors [i.e., other than the customer being a beneficiary of a life insurance policy, applying for citizenship in exchange for assets or the transaction relates to oil, arms, precious metals, tobacco, cultural artefacts, etc.] for enhanced due diligence, set out in regulation 33 of the MLRs, which you consider to be not useful at identifying suspicious behaviour?

EMA response:

1. We think that the UK's current approach to EDD under the MLRs is a significant cause of additional regulatory compliance burden disproportionate to the ML/TF risk, affecting the UK's competitiveness. It should therefore be adjusted accordingly to a more risk-based approach. Whilst allowing for a risk-based approach to domestic PEPs is a clear step in the right direction, the following changes should also be made:
    a. We think that in its current form, the list of factors for the application of enhanced due diligence is overly prescriptive and would benefit from being moved to guidance, where it could be considered by obligated entities within a wider context of risks and be updated more frequently in line with industry developments. For example, both the factors referring to non-face-to-face business relationships and to new technologies are now outdated given that most business relationships are established online and new technologies are widely employed to limit risks, including ML/TF risks.
    b. Any factors or measures that go beyond FATF standards should be removed.
    c. Industry should be encouraged to develop guidance as to relevant risk factors to be considered, not simply to be taken into account (so giving firms the ability and confidence to determine the right approach for them, reflecting their own ML/TF risk assessments).

High Risk Third Countries

Q16: Would removing the list of checks at regulation 33(3A), or making the list non-mandatory, reduce the current burdens (cost and time etc.) currently placed on regulated firms by the HRTC rules? How?

EMA response:

1. Moving to a risk-based approach and removing the list of checks in regulation 33(3A) (or at least making the list non-mandatory) would significantly reduce the current burdens (both cost and time) currently placed on regulated firms by the HRTC rules. The list of checks goes over and above FATF requirements and stifles firms' ability to apply more effective enhanced measures (e.g., based on sophisticated machine learning, which draws on the risks posed by the customer and each firm's unique business model rather than merely applying a list) whilst time is spent implementing the mandatory checks that yield little tangible benefit.

Q18: Are there any High Risk Third Country-established customers or transactions where you think the current requirement to carry out EDD is not proportionate to the risk they present? Please provide examples of these and indicate, where you can, whether this represents a significant proportion of customers/transactions.

EMA response:

1. Some of members provide payment services to customers based in high-risk jurisdiction that are, for example, offering goods or services for sale. The move of funds is here closely linked to the underlying product or service (such as a holiday let), which is separately ascertained as being genuine. In this respect, the customer's location in a high-risk jurisdiction does not itself indicate a higher risk. Without the presence of further (often business-specific) risk factors, EDD may therefore not be warranted. For some of our members, such customers represent a significant portion of their customer base.

Q19: If you answered yes to the above question, what changes, if any, could enable firms to take a more proportionate approach? What impact would this have?

EMA response:

1. The FATF has made clear its view that jurisdictions on its 'Increased Monitoring' (grey) list should not automatically result in the application of EDD (see FATF's circular issued October 2023[1]). Instead, the FATF expects members to adopt a risk-based approach in relation to such countries and not to apply blanket measures by de-risking or cutting off entire classes of customers. Regulation 33(3)(a)(ii) expressly precludes such an approach and mandates the application of EDD in relation to any customer who is associated with a country on the grey list. This is against FATF's objectives and is disproportionate to the risk.
2. For customers based in countries on the FATF grey list, firms should be allowed to implement a phased approach. The list is published three times a year and can result in whole segments of customers being re-classified effectively overnight. For firms operating

[1] https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-october-2023.html

globally, it is simply not possible to implement the additional measures required by EDD in such a short space of time, and in reality, this often leads to large backlogs and customer friction. The ML/TF risk of a customer does not change overnight when a country is designated by the FATF, and a phased approach would allow for continued economic activity.

Simplified Due Diligence

Pooled client accounts

Q22: In circumstances where banks apply SDD in offering PCAs to low-risk businesses, information on the identity of the persons on whose behalf funds are held in the PCA must be made available on request to the bank. How effective and/or proportionate do you think this risk mitigation factor is? Should this requirement be retained in the MLRs?

EMA response:

1. In relation to PCAs: While safeguarding accounts of EMIs and PIs are not currently treated as pooled client accounts, they may be so treated in the future, in which case the same considerations as for other pooled client accounts will apply. Given the difficulties EMIs and PIs face already today in obtaining safeguarding accounts, we strongly support the retention of SDD provisions to lower the associated compliance costs for banks and keep the duplication of CDD requirements to a minimum.
2. In relation to SDD more generally, we would advocate a much broader scope for applying SDD than is currently permitted under the MLRs, allowing firms to take into account for their own risk assessments a much broader set of customer-related and transaction-related low-risk factors. For example, the ability to apply SDD could be expanded, such that SDD may be applied upon establishment of a business relationship, with a firm required to apply CDD only on a risk-based approach thereafter, e.g., when firm-identified monetary thresholds are reached, or indicators of higher risk are identified. This would allow easier initial on-boarding of a customer, while deferring the friction of CDD to when risk arises and when a customer better understands the need for CDD information requests (because the ML/TF risk is more obvious) and is therefore more motivated to deal with the CDD information requests at that time.

Q24: Do you agree that we should expand the regulation on reliance on others to permit reliance in respect of ongoing monitoring for PCA and equivalent scenarios?

EMA response:

1. We support expanding the regulation on reliance to include ongoing monitoring. E-money and payments occur rapidly, with transfers in and out of safeguarding accounts often reflecting periodic settlements rather than the movement of individual client funds. EMIs and PIs are therefore best-placed to conduct monitoring of individual transactions through their internal systems. Only they have the needed oversight, information and business-specific know-how do determine suspicious activity in the e-money or payments context.
2. However, as a more general point we consider that the application of reliance provisions is overly burdensome where both obliged entities are regulated financial institutions. Reliance

still requires the relying party to have overall responsibility for CDD, effectively duplicating the responsibility of the institution relied upon. Banks holding pooled client accounts for another financial institution should only need to monitor for departures from expected transaction patterns for the account itself (such as sudden rises or falls in the overall balance), which could suggest illicit activity by the account holder.

Currency Thresholds

Q36: In your view, are there any reasons why the government should retain references to euros in the MLRs?

EMA response:

1. Given that many of our members operate in more than one jurisdiction, it would be helpful to retain euro thresholds where these respond directly to FATF requirements. For any UK-only requirements, pounds sterling is the preferred denomination.

Q39: If the government were to change all references to euros in the MLRs to pound sterling which of the above conversion methods (Option A or Option B) do you think would be best course of action?

EMA response:

1. If thresholds are converted into pound sterling, our members would prefer Option A, i.e., conversion on a 1:1 basis.

Change in control for cryptoasset service providers

Q44: Do you agree that the MLRs should be updated to take into account the upcoming regulatory changes under FSMA regime? If not, please explain your reasons.

EMA response:

1. It would be helpful to understand exactly what firms will remain under the MLR registration regime once the FSMA regime comes into force.
2. The question also arises why the change of control regime for MLR-registered firms needs to be as stringent as for those regulated under FSMA, given the former are unlikely to offer services of a financial nature. Cryptoasset firms falling under FSMA and remaining under the MLRS are not necessarily in the same industry, with business cases and intended customer bases likely to diverge widely. The fact that the proposed changes will allow some firms to transition more easily to the FSMA regime once this applies is not a sufficient reason to change the regime for all MLR-registered firms, including those who will never transition to FSMA. Such firms should not be singled out merely because they offer cryptoasset-related services. They should be treated like other non-financial firms regulated under the MLRs.

Q45: Do you have views on the sequencing of any such changes to the MLRs in relation to the upcoming regulatory changes under the FSMA regime? If yes, please explain.

EMA response:

1. If the proposals are adopted, any changes to the MLRs should be aligned with timelines of the FSMA regime and offer appropriate transitional provisions to allow firms to prepare for the more stringent FSMA change in control regime.

Members of the EMA, as of June 2024

Airbnb Inc
Airwallex (UK) Limited
Allegro Group
Amazon
Ambr
American Express
ArcaPay UAB
Banked
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network EMEA Limited
Boku Inc
Booking Holdings Financial Services International Limited
BVNK
CashFlows
Circle
Coinbase
Contis
Crypto.com
Currenxie Technologies Limited
Decta Limited
eBay Sarl
ECOMMPAY Limited
Em@ney Plc
emerchantpay Group Ltd
EPG Financial Services Limited
eToro Money
Etsy Ireland UC
Euronet Worldwide Inc
Facebook Payments International Ltd
Financial House Limited
First Rate Exchange Services
Flywire
Gemini
Globepay Limited
GoCardless Ltd
Google Payment Ltd
IDT Financial Services Limited
iFAST Global Bank Limited
Imagor SA
Ixaris Systems Ltd
J. P. Morgan Mobility Payments Solutions S. A.
Lightspark Group, Inc.
Modulr Finance B.V.
MONAVATE
MONETLEY LTD
Moneyhub Financial Technology Ltd
Moorwand Ltd
MuchBetter
myPOS Payments Ltd
Navro Group Limited
Nuvei Financial Services Ltd
OFX
OKG Payment Services Ltd
OKTO
One Money Mail Ltd
OpenPayd
Own.Solutions
Park Card Services Limited
Payhawk Financial Services Limited
Paymentsense Limited
Paynt
Payoneer Europe Limited
PayPal
Paysafe Group
Paysend EU DAC
Plaid
PPRO Financial Ltd
PPS
Push Labs Limited
Ramp Swaps Ltd
Remitly
Revolut
Ripple
Securiclick Limited
Segpay
Soldo Financial Services Ireland DAC
Square
Stripe
SumUp Limited
Syspay Ltd
Transact Payments Limited
TransferGo Ltd
TransferMate Global Payments
TrueLayer Limited
Uber BV
VallettaPay
Vitesse PSP Ltd
Viva Payments SA
Weavr Limited
WEX Europe UK Limited
Wise
WorldFirst
Worldpay
Yapily Ltd