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

General Secretariat of the Treasury
and International Financing

Submitted by email to:
secretarialCMC@economia.gob.es

23 June, 2020

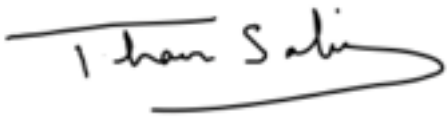
Dear Sir/Madam,

Re: Consultation on the draft law amending Ley 10/2010 of 28 April, on the prevention of money laundering and terrorist financing implementing the Fifth Money Laundering Directive ("5MLD")

The Electronic Money Association is the trade body for electronic money issuers and innovative payment service providers. Our members include leading payments and e-commerce businesses worldwide, representing online payments, card-based products, vouchers, and those employing mobile channels of payment. Please find full list of our members attached to this letter.

Below we provide some detailed comments with regard to the proposed implementation of 5MLD in Spain.

Yours faithfully



Thaer Sabri
Chief Executive Officer
Electronic Money Association

1. Requirement to register for virtual currency service providers

Approach proposed in the consultation: the requirement to register applies to virtual currency service providers providing services to residents in Spain, which includes those providing services cross-border.

EMA response: EU AML legislation is largely applied on the basis of establishment, with the expectation that home member state supervisors share information and intelligence with host member states as and when required. This avoids the situation where cross-border service providers have to obtain registration or a licence in all 27 member states.

Virtual currency exchange (virtual to virtual and crypto to fiat exchange) and custodian wallet providers are obliged subjects also where they are not established in Spain in line with the position regulated financial institutions. Virtual currency providers therefore have to comply with the same AML requirements as financial service providers and are subject to the same reporting requirements and compliance obligations. They should therefore not be subject to registration requirements that do not apply to financial service providers. We would therefore urge you to reconsider the application of the registration requirement to virtual currency service providers providing services on a cross-border basis, and to limit the application to those providers that are established in Spain.

The growing tendency for host member state regulation is at variance with the principles of harmonisation, the single market and the freedom to provide services without additional barriers. It is also an inefficient way to address AML data sharing, creating a significant burden on firms.

Furthermore, the European Commission is developing an EU-wide framework for regulating virtual currency service providers in order to deliver a harmonised regime across EEA member states.

2. AML obligations for firms using distributors (Article 26(1)-(3))

Approach proposed in the consultation: requirement for PSPs operating in Spain through agents or forms of **permanent establishment** other than a branch to appoint a representative resident in Spain, who will be considered a central contact point.

EMA response: the appointment of a representative or a contact point ("**CCP**") must be predicated on the distributor being established (Recital 50, Article 45(9), 4MLD)[1] in the host member state; if there is no establishment, then then there are no grounds for a CCP.

The purpose of the representative is to help SEPBLAC communicate and coordinate compliance-related matters with the passporting firm. The need for a representative should therefore be related to the extent of the activity undertaken by the distributor or agent.

This means a distributor that is simply selling prepaid cards for example, and not redeeming e-money, not providing customer service, not undertaking CDD processes, would be less likely to give rise to a need for a CCP, even if established. This is because the activity undertaken in Spain in the course of establishment would not give rise to sufficiently broad issues to warrant the cost of placing a CCP. Distribution of e-money does not usually involve the offering of a regulated service; it neither involves issuing e-money (an activity that takes place within the system of the issuer), nor the provisions of a payment service (this takes place when the e-money product is used to make a payment, and again takes place within the system of the issuer). Furthermore, all compliance related matters will be dealt with by the home-based issuer, and the issuer is in a better position to address queries.

The cost of requiring a local point of contact for each issuer that physically distributes products in Spain will be prohibitive, and will discourage iterative growth of the industry across member states.

3. Establishment of address in Spain and representative (Article 26 ter)

[1] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L0849

Approach proposed in the consultation: Cross-border service providers must nominate a representative to SEPBLAC. The representative does not have to reside in Spain but may be based at the head office, but the firm must have an address in Spain for communication and notification purposes.

EMA Response: It is unclear what are the benefits – either to SEPBLAC or to obliged entities – of requiring firms offering cross-border services to have an address in Spain. We understand that the representative will act as a transmitter of information, and non-response to a request by SEPLAC or the Treasury may result in a fine against the firm. In practical terms this will likely require firms to appoint a physical representative who can be entrusted with the role of transmitting information requests and responses on behalf of the firm, thus increasing the cost and administrative burden on firms with no real benefit. Many firms will be dissuaded from serving Spanish customers because of the costs associated with setting up such a representative, and Spanish customers will not be able to benefit from the services offered by Fintech firms to consumers in other EEA Member States.

At present, firms operating on a cross- border basis nominate a permanent representative based at the head office, usually the Money Laundering Reporting Officer ("MLRO"). As part of the nomination of the permanent representative, the MLRO's contact details are communicated to SEPBLAC and these have to be kept up to date.

The purpose of the representative appears to be to help SEPBLAC communicate and coordinate compliance-related matters with the passporting firm. As most compliance, monitoring and other AML-related functions are conducted by the entity in the home Member State, it would be better to make direct contact with the MLRO at the head office where access to all internal systems and data is available.

The compliance officer or MLRO could therefore provide a convenient point of engagement without adding unnecessary cost. Particularly in this digital age where most communication is over email and phone, the physical location of a representative should be irrelevant, and the requirement to have a physical postal address unnecessary.

4. External review of policies and internal controls (Article 28)

Approach proposed in the consultation: external experts that annually review the PSP's policies and internal controls, will have direct responsibility for the content of the reports under the AML law.

EMA response: it is unclear how this requirement will add value to the current regime.

Instead the requirement may lead to the number of firms offering such a service to reduce, as only firms willing to be subject to the requirements of Spanish AML law, including the obligation to notify SEPBLAC and report on a six-monthly basis, will continue to offer such services. Firms that currently have technical expertise in payments, fraud, technology and finance may withdraw their services. This will have a particularly detrimental impact on smaller PSPs, as the cost of appointing such auditors may increase as the number of firms able to offer the necessary technical expertise and knowledge reduces.

Cross-border service providers that have a little over 10 employees and an annual turnover or balance sheet exceeding €2m, but limited footprint in Spain may suffer the consequences of the cost of these services disproportionately, and thus withdraw their services from Spanish customers. For such providers there should be a more informal process in order to provides assurances for Internal audit and / or the compliance function.

5. Implementation of the IBAN database – Financial Ownership File (Article 43)

Approach proposed in the consultation: CIs, EMIs and PIs must declare to SEPBLAC opening and cancellation of checking accounts, savings accounts, deposits **and any other type of payment accounts**, as well as safe deposit box rental contracts and their period of lease, regardless of its commercial name. Reporting frequency will be determined in forthcoming regulations.

EMA response: Obliged entities in scope of the law include not only PSPs authorised in Spain or providing services in Spain through a branch or agent but also those providing services on a cross-border basis. Such cross-border providers are already subject to the home member state reporting requirements in relation to payment accounts associated with an IBAN under the local 5MLD implementing legislation.

Applying this provision to such PSPs would therefore result in multiple reporting obligations, for the same account, in at least two member states. The reporting formats are likely to differ, as will the timelines. We believe the application of this obligation to cross-border service providers is disproportionate and acts to erode the benefits of the European Single Market. It may in some circumstances, where the volume of business does not justify the cost for these firms, lead them to withdraw their offerings in Spain.

We also note that the expanded reporting obligation appears to apply to **all** payment accounts, including those not identified by an IBAN. However, 5MLD (Article 32a 1) stipulates that the central register should allow the identification natural or legal persons holding or controlling payment accounts and bank accounts **identified by IBAN.**

Accounts that are not identified by an IBAN should therefore not fall within 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 5MLD. 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. Low value, or 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 gift voucher/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 directly through the permanent representative based at the head office.

6. Common information storage systems for CDD information (Article 32 bis)

Approach proposed in the consultation: new provision allowing creation of a common information storage systems for CDD information, reflecting the evolution of technological innovations to improve compliance with the legal obligations of the obligated subjects. Obliged entities belonging **to the same category** may create common information, storage and access to the information and documentation collected for compliance with the CDD obligations. Maintenance of these systems may be entrusted to a third party, which is not required to be an obliged entity. Co-responsible obliged subjects must notify the Prevention Commission of ML and Monetary Offenses the intention of constituting these systems at least 60 days before it is put into operation.

EMA response: we welcome the introduction of this provision allowing establishment of the CDD information database, which utilizes new technical capabilities and has potential for reducing costs and enhancing compliance with the AML obligations.

However, the restriction of access to obliged entities within the same category should be reconsidered. In order to benefit from efficiencies in the marketplace, and to ensure a level playing field, such databases should not be designed along the lines of category of entity, but rather by function. For example, all firms providing payment or banking services should be able to contribute to, and access, the same database, regardless of whether they are a credit institution, a payment institution or an e-money institution. Otherwise, this will create an unfair competitive advantage for firms in one category over those in another with whom they are in competition e.g. credit institutions will have an advantage over smaller industry participants such as e-money and payment institutions.

7. Politically Exposed People (PEPs) (Article 14(2))

Approach in the consultation: The draft proposes that people in senior management at regional or local political party representations where there are more than 50,000 inhabitants are included in the definition of PEP.

EMA response: The addition of this new category of individuals within the definition of a PEP will place a considerable additional burden on firms, as it will significantly increase the number of customers subject to Enhanced Due Diligence.

The burden is further exacerbated by the constant change within regional and local politics in Spain, and the limited data available regarding the identity of senior officials of political parties. One option to mitigate the burden would be to create a national list of PEPs that is machine-readable and accessible to obliged entities to consult when conducting KYC on new customers.

8. Customer identification – acceptable documentation

Approach in the consultation: The draft only mentions the national ID document as reliable for the purposes of identification.

EMA response: Driving licences and passports should also be considered reliable forms of identification in addition to the national ID card, as their use for the purposes of identification and verification is not excluded under 5MLD, and is accepted by FATF Recommendations.

Article 13.1(a) 5MLD does not exclude the use of passports or driving licences, and requires obliged entities to "*identify the customer and verify his identity on the basis of documents, information or data obtained from reliable and independent sources, including, where available, electronic means of identification, relevant trusted services within the meaning of Regulation (EU) No 910/2014 of the European Parliament and of the Council (*) or any other secure remote or electronic identification process, which have been regulated, recognized, approved or accepted by the competent national authorities*". In fact, Financial Action Task Force (FATF) Recommendation 11 considers passports and driving licenses as valid documents to carry out due diligence.

The Spanish legal system permits the formal identification of individuals using a passport, so it seems inconsistent not to allow this form of identification for the purposes of AML-TF compliance. Article 11.1 of Organic Law 4/2015 of 30 March on the Protection of Citizen Security recognizes that the Spanish passport is an identification document valid both abroad and within Spain. Article 6.1(a) paragraph II of Royal Decree 304/2014 allows for the use of passports for the identification of foreign citizens.

Driving licences should also be considered valid identification for KYC purposes. According to Article 7.1 of Royal Decree 818/2009 of 8 May approving the General Drivers Regulations, in order to apply for a permit or driver's license, residency of at least six months must be established, and verification of other reliable ID documentation must be completed. At EU level, discussions about moving towards the use of plastic driving licences were predicated on the fact that they are used as valid ID documents. EU Directive 2006/126/EC on the driving license requires driving licenses to include the name and surname of the holder, date and place of birth, date of issue of the permit, designation of the issuing authority, the permit number, photograph and signature of the holder.

List of EMA members as of June 2020

AAVE LIMITED
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
Curve
eBay Sarl
ECOMMPAY Limited
Em@ney Plc
ePayments Systems Limited
Euronet Worldwide Inc
Facebook Payments International Ltd
First Rate Exchange Services
Flex-e-card
Flywire
Gemini
GoCardless Ltd
Google Payment Ltd
IDT Financial Services Limited
Imagor SA
Intuit Inc.
Ixaris Systems Ltd
Modulr FS Europe Limited
Moneyhub Financial Technology Ltd
MuchBetter
myPOS Europe Limited
Nvayo Limited
One Money Mail Ltd
OpenPayd
Optal
Own.Solutions
Park Card Services Limited
Paybase Limited
Paydoo Payments UAB
Payoneer
PayPal Europe Ltd
Paysafe Group
Plaid
PPRO Financial Ltd
PPS
QIX Ltd
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
Valitor
Vitesse PSP Ltd
Viva Payments SA
WEX Europe UK Limited
Wirecard AG
Wirex Limited
WorldFirst
Worldpay UK Limited
WorldRemit