CONFIDENTIAL

To: Lithuanian Ministry of Finance, Bank of Lithuania

From: Dr Thaer Sabri, Electronic Money Association (EMA)

Subject: Lithuanian 5MLD implementation

Date: 14 January 2019

The EMA would like to make the following comments and suggestions in relation to Lithuania's proposed implementation of the 5th Money Laundering Directive (5MLD) through Law VIII-275:

1) We note that **the e-money exclusion from customer due diligence (CDD)** in Article 9(4) is more restrictive in Lithuanian law than in the Directive. The latter allows the application of the exclusion to non-reloadable products that can be used outside the relevant Member State, while Lithuanian law does not. This allowance is important if Lithuanian e-money issuers are to passport their services across the EU. We therefore request that the legislator consider widening this provision to include use in other EU member states.
2) We would like to make the following suggestions for amendment of **the simplified due diligence (SDD) provisions for e-money** in Article 15(1)(7) so as to make these provisions more useful to the e-money industry located in Lithuania. In their current state, these provisions only provide a limited exception from full verification requirements for products whose risk profile would warrant a wider exception. Therefore, we suggest that parameters are specified within which products may make use of the SDD provisions beyond the EUR 1,000 limit.

3) In this respect, we recommend a higher annual limit of EUR 2,500 to also be provided for, which would be available if the product met ANY of the following conditions:
    a. Where the e-money instrument may only be used to purchase goods or services and no more than EUR 500 can be withdrawn in any 12 month period.
    b. Where the product allows for person to person payments, as well as the purchase of goods and services, but does not allow for any cash funding or

cash withdrawal to be undertaken.

4) It would also be helpful if the account referred to in Article 15(2)(2) could be extended to a verified account with any regulated payment service provider so as to include, for example, non-bank issuers of credit cards that have been subject to CDD.

5) It is not clear why Article 15(1)(7) excludes products that fall within the Article 9(4) from benefiting from SDD. If a product meets SDD criteria, it should be able to take advantage of the SDD provisions.

   This is because SDD provisions require the identification of the customer, going beyond the requirements of Article 9(4). The 4MLD text provides for such situations under Recital 7; which states:

   "Such an exemption should be without prejudice to the discretion given to Member States to allow obliged entities to apply simplified customer due diligence measures to other electronic money products posing lower risks, in accordance with Article 15."

   It has for example been implemented in UK legislation; see Regulation 38(4) of the UK Money laundering Regulations 2017.

6) We also propose to add to Article 15(1)(2) institutes of education and institutes of health, as also meriting consideration as low risk

7) Finally we propose that the requirement under SDD Article 15(2)(2) for the first payment to be from an account with a credit institution, for this to be broadened to allow other payment service provider accounts to be relied upon, provided they have been subject to CDD verification in accordance with EU law.

8) The means of conducting **CDD in a non-face-to-face environment** that the Lithuanian law provides under Article 11 are not suitable for low-value payment products where the risk is low, as they are difficult and costly to implement.

We propose amending the law to include the following additional means of conducting CDD; these fall within the requirement to verify identity on the basis of documents, data or information obtained from a reliable and independent source, and could additionally be made subject to a cumulative lifetime turnover limit of EUR 10,000:

a. Verification of identity by reliance on the funding instrument: as part of a risk-based approach to verification of identity, e-money issuers may rely in situations of low risk on the customer's funding instrument to establish their identity. This may happen only where funds to purchase electronic money are drawn from an account held with a credit or financial institution in the EU or an equivalent jurisdiction and which is supervised for its AML controls. The issuer would continue to retain ultimate responsibility for the verification of identity undertaken through this means and must implement systems and controls to mitigate the risk of the funding account being itself subject to SDD or the e-money exclusion from CDD.

   Furthermore, the issuer would have to establish that the customer has control over the account from which the funds are drawn. This can be done in a number of ways, including the following:

   i. Micro-deposit: A small random amount of money is credited to a customer's funding account and the customer is then required to discover the amount and to enter it on the issuer's website. By entering the correct value, the customer demonstrates access to the bank/card statement or accounting system of their bank or financial institution.
   ii. Additional data checks: issuers may also use additional data checks undertaken at the time of the transaction which seek to verify that the account is under the control of the customer, by accessing the customer's account directly (for example acting as an Account

Information Service Provider) or from an independent third party.

iii. Requiring the customer to execute strong customer authentication against the funding account can also serve to demonstrate control over the account.

iv. Evidence of legitimate use: An account that is used to fund an electronic money purse over a significant period of time is more likely to be used legitimately, as the passage of time gives the rightful owner the opportunity to discover fraudulent use of the product and to block its use or initiate a chargeback, which would in turn become evident to the issuer. A minimum period of four months must elapse, together with significant usage in terms of number and value of transactions over this time, to satisfy the issuer that the instrument is being legitimately used.

b. Verification of aspects of the customer's identity on the basis of detected data or information: for example, as part of a risk-based approach to verification of address, e-money issuers may rely in situations of low risk on the geolocation of the customer's login IP addresses when undertaken over a period of time to verify the customer's address. While IP geolocation cannot be attributed to an exact address, the detection of IP addresses over a period of 2-3 months for example will provide sufficient data for a view to be taken on the accuracy of the submitted address information. Issuers will have to apply measures to ascertain that the IP data is reliable. This can be achieved through a range of measures including through (the existing) identification of VPN service usage or through the development of patterns of fraudulent behaviour from ongoing monitoring.

c. Other similar sources of data could be the geolocation of a mobile phone handset, again over a significant number of occasions.