



Electronic Money Association

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

9 February 2018

Dear Mr. Euclid Tsakalotos
Ministry of Finance
Nikis 5-7, Athens 10562, Greece

**Re: EMA comments on the 4th EU Anti-Money Laundering Directive-
ΠΡΟΛΗΨΗ ΚΑΙ ΚΑΤΑΣΤΟΛΗ ΤΗΣ ΝΟΜΙΜΟΠΟΙΗΣΗΣ ΕΣΟΔΩΝ ΑΠΟ
ΕΓΚΛΗΜΑΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ ΚΑΙ ΤΗΣ ΧΡΗΜΑΤΟΔΟΤΗΣΗΣ ΤΗΣ
ΤΡΟΜΟΚΡΑΤΙΑΣ**

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, and mobile payment instruments. 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.

The EMA welcomes the opportunity to provide comments to the Ministry of finance on its implementation of customer due diligence and local point of contact provisions in the fourth Money Laundering Directive.

I would be grateful for your consideration of our comments and proposals.

Yours sincerely,

Dr Thaeer Sabri
Chief Executive Officer
Electronic Money Association

EMA Comments

4MLD Article 12: Exemption from CDD for some e-money products

The industry strongly encourages the implementation of the Article 12 discretion, and supports the holistic approach taken by the European Supervisory Authorities (“ESAs”) in identifying risk factors relevant to e-money products. Currently 93% (Equalling 98m cards) of all e-money cards and vouchers issued in the EEA benefit from simplified due diligence under the 3rd Money Laundering Directive; it is vital for the industry that this allowance continues to be available.

Article 12 allows elements of customer due diligence (‘CDD’) to be suspended within very low value transaction and turnover limits - (customer and transaction monitoring continue to be required). This is an implementation of the risk-based approach, enabling convenient access to products by consumers.

Users of e-money have indicated an unwillingness to undergo up front verification of identity where low value transactions are involved, and for low value payment instruments generally.¹ Cards are mostly sold in retail locations, and retailers have neither the know-how nor the ability to introduce such processes to their stores. Users are similarly unwilling to reveal personal data within a supermarket setting or in small retail outlets.

This is because the friction introduced by the CDD step at the point of purchase of a low value payment product, or shortly thereafter is not regarded by consumers as justified given the limited use they are making of the product. It is unlike the process of opening a bank account for example, which is likely to play a central role in their financial interactions. A prepaid card or voucher on the other hand will be used in a limited manner and given the limits imposed for very limited transactions.

By removing barriers to the take-up of e-money by consumers as well as retailers, the suspension of CDD aids the increased adoption of electronic payment methods and thereby the displacement of cash activity within the economy. This displacement is the clear intention of the FATF, and functionality limitations and value thresholds achieve this outcome within defined risk parameters that limit the attractiveness of the product to money laundering or terrorist financing.

The transaction monitoring required in article 12(e) mitigates residual risk, as it allows unusual activity that may indicate an increase in risk to be detected. Compared to cash, e-money offers significant visibility of transactions and consequently generates information that can be made available to law enforcement.

E-money products also play an important role in financial inclusion by providing access to online commerce to persons who are not able to gain such access through traditional payment products.²

¹ The EMA’s experience is that the take-up of products drops in excess of 50% where CDD information is requested.

² The FATF has been critical of a one-fits-all approach to CDD requirements in its 2013 guidance on *Anti-Money Laundering and Terrorist Financing and Financial Inclusion*: ‘While the 2003 FATF Recommendations were also intended to encourage countries to apply an RBA, and did impose certain RBA related obligations, a review of the results of countries’ assessments carried out between 2005 and 2011 (among the FATF and the FSRBs community) shows that very few countries took full advantage of this flexibility. Rather, most countries have introduced a uniform approach with the same AML/CFT requirements applicable to all financial institutions,

Given the prevalence of cheaper products and services online, this is particularly significant for those whose financial exclusion goes hand in hand with limited means.

In summary, the e-money products that would benefit from the Article 12 allowance are limited in functionality, limited in the value of funds that can be transacted, and offer a number of advantages for both users and law enforcement. There has not, to our knowledge, been any systemic or significant vulnerabilities that have enabled the abuse of products subject to SDD or exemption for either money laundering or terrorist financing. We do not think this provision creates any significant vulnerability, and its exclusion would be a disproportionate reaction that will impact legitimate use of these products.

4MLD Article 45 (9): The option to require a central contact point for e-money issuers or other payment service providers passporting into Greece (Άρθρο 36 – Εσωτερικές διαδικασίες σε επίπεδο ομίλου)

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

Distribution of e-money does not 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).

Therefore, distributors have very little insight into the use of the e-money or the user profile, as they can only see their own customers purchasing e-money, and cannot see any of the spending of the value. They cannot see how the product is used, where, or how frequently, and can deduce very little about the customer. Rather, the issuer has oversight of the product as a whole, its issuance, funding, frequency and location of use, and which has the ability to impose controls, to authorise and to refuse transactions. It also has sight of merchant acceptance and distributor sales, so is able to monitor, manage risk and report suspicions to the FIU.

For this reason it would be better to make use of a contact point within the issuer's business where access to all internal systems and data is available. In this respect, the firm's compliance officer or MLRO is usually best placed, as he or she is the most knowledgeable about the product and the relevant compliance requirements. The compliance officer or MLRO could therefore provide a convenient point of engagement with the issuer without adding to cost unnecessarily.

clients, products and services. This may have hampered financial inclusion efforts of financial providers. At the customer level, customers who conduct limited and small value (potentially lower risk) financial transactions must often meet the same customer due diligence requirements as higher risk customers who frequently conduct large transactions.'

4MLD Article 26: Performance by Third Parties- Άρθρο 19 – Εφαρμογή μέτρων δέουσας επιμέλειας από τρίτα μέρη

We note that Article 19 of the draft Greek law implements Article 26 of 4MLD, and sets out a list of entities referred to as "third parties". We note that Electronic Money Institutions are not included in this list, and would request that they be included, as it may be disruptive to business, and there is no justification for excluding them from being considered "third parties" under Article 25 and 26 of 4MLD.

List of EMA members as of February 2018:

Advanced Payment Solutions Ltd
Airbnb Inc
Allegro Group
American Express
Azimo Limited
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network Ltd
Boku Inc
CashFlows
Citadel Commerce UK Ltd
Coinbase
Corner Banca SA
Ebanx
eBay Europe Sarl
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
Merpay Ltd.
MuchBetter
Nvayo Limited

One Money Mail Ltd
Optal
Park Card Services Limited
Paybase Limited
Payoneer
PayPal Europe Ltd
PayPoint Plc
Paysafe Group
PPRO Financial Ltd
PrePay Solutions
R. Raphael & Sons plc
Remitly
SafeCharge UK Limited
Securiclick Limited
Skrill Limited
Starpay Global Ltd.
Stripe
Syspay Ltd
Transact Payments Limited
Transact24 (UK) Ltd
TransferWise Ltd
Uber
Valitor
Vitesse PSP Ltd
Viva Payments SA
Wave Crest Holdings Ltd
Wirecard AG
Wirex Limited
Worldpay UK Limited