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

Jonathan Ryder
Head of Anti-Money Laundering Policy
Sanctions and Illicit Finance
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ

6 November 2015

Dear Jonathan,

Re: Review of the impact on business of the current anti-money laundering & terrorist financing regime

The Electronic Money Association (EMA) welcomes the opportunity to respond to the Cabinet Office's review of the impact on business of the current anti-money laundering (AML) and counter terrorist financing (CTF) regime, as e-money and other small value retail payment products are disproportionately impacted by some AML and CTF obligations.

The EMA is the trade body for electronic money issuers and innovative payment service providers including payment institutions, banks and payment schemes. The EMA has been privy to the evolution of innovative payments for over 13 years - from small niche offerings to a growing sector that is offering alternatives for payments to consumers and businesses alike. We operate across the EEA and often engage with regulators globally.

We have focused mainly –but not exclusively, on customer due diligence provisions, as these have the greatest impact on customer recruitment, and access to new payment products by consumers, and in some cases small merchants alike.

Yours sincerely,

Dr Thaer Sabri

Chief Executive Officer

Electronic Money Association

The EMA's Response

1. Customer Due Diligence (CDD)

This seeks to deter money laundering by requiring customers to be identified and for their identity to be verified. This is undertaken before the start of a business relationship. Whilst the obligation is in most instances reasonable, its implementation in practice and the timing of its application can give rise to significant barriers for business. (i) The first of these barriers relates to the cost of verifying a customer's identity at the outset; this can be prohibitively expensive when the value of the relationship is still unclear. (ii) Secondly the requirement to verify up-front can create a resistance to take-up and significant drop-off rates are experienced. (iii) Finally, the evidence of ID that is conventionally sought and accepted is largely drawn from traditional face-to-face interactions. It does not contemplate new sources of information that are available with online transactions, and for online modes of engagement.

The current AML/CTF regime allows for some flexibility, but there is a risk of this being drastically reduced in the upcoming Fourth Money Laundering Directive (4MLD), and particularly as a result of a disproportionate restriction introduced by the EBA in their role as issuers of Guidelines in relation to Article 17 and 18(4) of 4MLD. Paragraph 124 of the draft Guidelines, which were published on 21 October 2015, proposes in relation to simplified due diligence to all but prevent postponement of verification of identity by introducing a lifetime limit of €250 before CDD must be undertaken, a reduction from the current annual limit of €2500. No rationale has been provided for this significant development, nor any basis for a perceived increase in risk to justify the change. It will however have a detrimental effect on business and take-up of innovative payment products across the EU.

Should these restrictions be carried, our members inform us that they would withdraw from a number of markets where the cost of CDD would make such instrument non-viable. These are frequently products that are of particular value to individual with limited access to financial services.

(i) Cost of up-front verification:

Verification has an associated cost, whether undertaken in a face-to-face environment or online using electronic data sources. In some member states where the availability of electronic data is limited, more traditional means of verification have to be employed. The cost in all cases will vary from €2 to €10 or more.

Given that most e-money products are used for transactions in the region of €30 or so, and given that the abandonment rates are high - with many products being used for only one transaction, the cost of verification becomes substantial. It can amount to 30% of the value of the transaction, and serves little purpose, as the risk of money laundering in these circumstances is negligible.

It would be better for the payment service provider if verification of ID can postponed to a time when the risk justifies the cost, and use of the product justifies the verification overhead. The risk can be mitigated up to this point by applying transaction limits, restricting product functionality and perhaps restricting withdrawals of funds.

This would then yield a more risk based, proportionate, business- and user-friendly regime.

(ii) Loss of business due to verification at the outset

Most e-money products are intended as low value payment products, and are used for specific purposes, often to cover an existing gap in the market not catered for by traditional PSPs. There

is therefore a need to make access to the products as easy as possible and to minimise barriers to take up. Requiring detailed identification and verification processes to be completed ahead of product use has been found to result in as much as a 50% drop-out rate. Users do not regard the utility offered by the products as justifying the kind of CDD process associated with opening a bank account. We make the point again that more onerous and less flexible CDD requirements will have a material impact on access to financial services by consumers that already suffer from financial inclusion challenges.

It is therefore again necessary to have a risk based approach to CDD, and more importantly for verification to be capable of postponement so that the steps necessary for completion of CDD can be undertaken once a user has experienced the benefits of the product, rather than before they have been able to use it.

A related experience is that of requiring CDD to be undertaken in a retail store environment, which is the means by which many card and voucher based products are distributed to consumers. In such situations a number of additional difficulties arise:

- Retailers do not wish to adopt processes that create delays at checkouts or customer service desks
- Many customers are unwilling to provide their ID at checkout due to privacy concerns (this is also top of mind because of recent high profile data breach events associated with non financial services businesses).
- Many retail outlets are not in a position to collect information or verify documents in a data protection-compliant manner. The cost and risk of doing so would outweigh the benefits of distributing e-money products.

This emphasizes the need for postponement, and an incremental process, of undertaking CDD.

(iii) Means of undertaking CDD

CDD comprises identification and then verification of the elements of identity, usually by reference to independent sources of information such as official identification documents or electronic records held by credit reference agencies or public registers.

Both physical and electronic verification seek to confirm that the name and address or date of birth are genuine by confirming that a person matching this data exists. A third check is then needed to establish that the proposed customer is in fact that person.

(a) In practice, the only viable means of verification is with reference to electronic sources of data, as the sharing of official documents when customers are remote is fraught with difficulties. Risks associated with sending original documents are high, and the process of authentication or notarization is cumbersome and time consuming. Furthermore, staff do not often have the requisite skill to distinguish genuine copies of documents from forgeries.

(b) Availability of reliable electronic data is however highly variable, with good sources in the UK for example, but far fewer in other EU member states, with a complete absence of such data in many member states. Completing CDD processes is therefore challenging, with the consequent impact on customer retention. This is a matter that would benefit from being pursued at an EU level and anything that UK government can do in this regard would greatly assist business and new payment providers.

(c) Additional barriers exist in some member states that do not yet recognize electronic records of identity as a sufficient means of evidencing identity and impose varied and inconsistent requirements. This gives rise to greater difficulties in completing CDD for customers based in these states. Again, this would benefit from an EU wide initiative aimed at removing such barriers.

2. Components that make up identity

An area on which we would like to place significant emphasis is what is accepted as sufficient in order to circumscribe the elements of identity on the one hand, and secondly what data can be obtained to evidence these components. We believe that name and/or date of birth should not be the only elements that are accepted for the purposes of meeting the requirements of CDD.

Our starting point is the objective of CDD in AML/CTF legislation, which is ostensibly to deter crime on the one hand, and to enable law enforcement to investigate, pursue and apprehend criminals on the other.

These objectives can be met by obtaining alternative components of identity. The use of CCTV for example is often an effective means of deterring crime, and also of tracking criminals. In an analogous manner, e-commerce transactions yield a wealth of data that can be used to identify and track users, often with greater degree of certainty than conventional name and address information.

Such information includes IP addresses, device ID, geo-location data, transaction patterns, delivery addresses, and data from online data collection agencies. Furthermore, where a payment service provider is associated with another e-commerce service, whether sales of goods and services, online digital services or services with a social network component, yet more data is available to mitigate risk and identify users.

This kind of data is far more difficult to falsify, and creates an online fingerprint that is unique to the user, and which in the event of a crime taking place can be used by investigators to identify and apprehend an individual.

Use of this type of information is at its infancy, but already enables many of our members to manage risk, detect incidents relating to a single or linked group of individuals, and provides a more reliable means of managing identity fraud.

It could therefore be helpful if this can be more formally recognized as a justified component of identification and verification for CDD purposes, and where the risk is low, as the predominant means of verification.

3. Home or host national risk assessment

A separate, but related issue is the **varied approaches adopted by different EU regulators when assessing the level of AML risk** posed by innovative digital financial services products. Under 4MLD, each Member State will undertake its own assessment of the AML risk associated with different products (Article 7), and this will determine the extent to which SDD can be applied.

Many of our members are based in the UK and passport to other EU Member States. It would be impossible to adopt the findings of 29 different risk assessments and to have such provisions reflected in the AML processes that are adopted for their different products. Some member states may also refrain from implementing SDD provisions altogether. The result will be that firms will either adopt the most onerous regime, or will seek to exclude a range of markets from their service offering. A more harmonized approach would increase certainty and reduce barriers to access within the EU market for both payments and other startup fintech providers. AML and TF risk is a pan EU issue that does not respect Member state borders. Our members firmly believe that a consistent and harmonized approach to CDD will have the effect of significantly improving the overall performance of CDD measures in terms of preventing or deterring money laundering and terrorist financing. Our members will then be able to focus more of their finite resources on the end results as opposed to the technical and administrative burden of meeting numerous divergent local requirements.

4. Local point of contact

Similarly, the 4MLD introduction of a requirement for a **local physical point of contact** (Article 45, para 10) where e-money is distributed in a host country is disproportionate and serves no practical purpose. All compliance information is usually held centrally with the issuer, who is based in the home Member State, and is better placed to assist with any questions or concerns from the regulator. Estimates from EMA members regarding the cost of setting up of local points of contact (i.e. identifying an appropriate person, setting up an office etc.) are in the region of €250,000, and ongoing running costs are at least €150,000 p.a. for each local contact point. This requirement has the potential to severely restrict access for startups to other EU markets. Further, it again detracts from the allocation of finite resources to meeting the true aims of AML and CTF regulations, preventing crime.

Whilst this obligation is now part of 4MLD, the EBA is charged with issuing Guidelines on the threshold for when it would apply. These are best set as high as possible to ensure minimum impact on small and growing businesses, and for this to be a more natural development, perhaps when a business has already grown to a point where it has established a base in a host member state and can therefore more naturally allocate such a resource.

List of EMA members as of November 2015:

Advanced Payment Solutions Ltd
Airbnb Inc
American Express
Azimo Limited
Blackhawk Network Ltd
Boku Inc
Citadel Commerce UK Ltd
ClickandBuy International Ltd
Clydesdale Bank
Corner Banca SA
Ekuantia EDE, S.L.
EMP Systems Limited
Euronet Worldwide Inc
Facebook Payments International Ltd
First Rate Exchange Services
Google Payment Ltd
iCheque Network Limited
IDT Financial Services Limited
Ixaris Systems Ltd
Kalixa Pay Ltd
Marq Millions Limited
One Money Mail Ltd
Optimal Payments
Park Card Services Limited
Payleven Ltd
Payoneer
PayPal Europe Ltd
PayPoint Plc
PayU
Paywizard
PPRO Financial Ltd
Prepaid Services Company Ltd
PrePay Technologies Ltd
PSI-Pay Ltd
Q Money Limited
R. Raphael & Sons plc
Securiclick Limited
Skrill Limited
Stripe Payments UK Limited
Syspay Ltd
Transact Payments Limited
TransferWise
Valitor
Wave Crest Holdings Ltd
Wirecard AG
Worldpay UK Limited
Yandex.Money