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

Ms Carolin Gardner
European Banking Authority
One Canada Square (Floor 46)
Canary Wharf
London E14 5AA
UK

22 January, 2016

Dear Carolin,

Re: EMA Response to ESA Consultation on Joint Guidelines under Article 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions

The Electronic Money Association ("**EMA**") welcomes the opportunity to respond to the consultation on the draft Guidelines on SDD and EDD and related risk factors ("**Draft Guidance**"). We are grateful for your willingness to receive and take our concerns into account.

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, representing online payments, card-based products, vouchers, and those employing mobile channels of payment, many of whom operate on a cross-border basis in the European Union ("**EU**"). A list of EMA members is given at the end of this letter.

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

Yours sincerely,

Thaer Sabri

Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

1. **Do you consider that these guidelines are conducive to firms adopting risk-based, proportionate and effective AML/CFT policies and procedures in line with the requirements set out in Directive (EU) 2015/849?**

We have found the guidelines helpful, informed and focused on the key areas of risk. We do however have a number of comments and have set these out in the paragraphs that follow.

Title I

2 Scope

Paragraph 2 sets out the scope of the guidance, and refers to Directive 2015/849 ("**4MLD**"). It suggests that firms may use the guidance when undertaking risk assessments under Article 8 4MLD. This is helpful, but extends the scope of Guidelines beyond the mandate of articles 17 and 18(4) 4MLD. The role of the Guidelines in respect of Article 8 obligations would therefore benefit from additional clarity, distinguishing any obligations placed on firms by the Guidelines in relation to this provision from those under Articles 17 and 18(4).

17 Risk factors

The holistic approach is supported, as is the statement that isolated risk factors do not necessarily move a relationship into a higher or lower risk category.

27

The third bullet refers to a firm's understanding of the risks associated with its products and services. This presumably relates to yet unknown risks associated with new products and services, rather than a firm's degree of understanding being a risk. Clarification would be helpful.

33-35 Weighting risk factors

This approach is welcome, as it provides for a more nuanced and meaningful process of risk assessment.

Clarification would however be welcome of bullet point 4 of paragraph **34**, which suggests that a firm cannot overrule the high-risk assessment in 4MLD or a national risk assessment. Presumably, this does not suggest that such risks cannot be mitigated and addressed. Having addressed such risks, it may be that the residual risk is reduced, and the overall assessment will be similarly impacted. It would help if this could be elaborated in the guidelines.

Please also see our comment under the section on PEPs below with regard to the same issue.

49 PEPs

The provision is overly complex, as it requires enquiries into both source of funds and wealth, senior management approval for both entering into and continuing relationships, and the level of seniority of management varying with the risk. Monitoring is required of both transactions and the 'risk', as well as the ongoing collection of information. All such provisions then need to be applied to PEPs, their family members and known close associates.

This could lead to the exclusion of many PEPs from financial services, as the cost of maintaining their accounts may outweigh any commercial benefit. Reference to a simplified approach where this is consistent with the risk posed would be helpful.

This can be addressed as part of the initial risk assessment. For example, the use of a EUR 250 prepaid card by a PEP or their associates is unlikely to give rise to the concerns associated with source of funds and source of wealth.

Alternatively, it may be that 4MLD Article 20(a), which requires 'risk based procedures to determine' whether a customer is a PEP in the first place provides sufficient flexibility to apply this requirement in a reasonable manner.

51-52 Correspondent relationships

Paragraph 51 elaborates on Article 19 of 4MLD, which requires additional CDD to be undertaken in relation to the business of a cross border third country correspondent relationship. This extends to an assessment of the correspondent's AML controls, and where 'payable-through' account functionality is offered, to ensure that customers of the respondent have been subject to CDD and ongoing monitoring, and that such information is available to the correspondent on request.

This requirement is borne from the need to ensure that equivalent levels of AML controls have been applied on the respondent's jurisdiction, and that customers of the respondent have been subject to comparable CDD processes.

This makes the provisions of paragraph 52 unusual, where they state: "these guidelines may also be useful for firms in other correspondent relationships." "Other correspondent relationships" is likely to be read as referring to relationships with other payment service providers that are NOT located in third countries; in other words to relationships with other institutions in the same jurisdiction.

This is problematic, as it could suggest:

(i) An obligation on the regulated institutions, requiring them to 'know their customer's customer'.
(ii) An outsourcing of supervisory responsibilities by the regulator to other financial institutions, requiring some to oversee the compliance performance of other regulated institutions in their member state
(iii) An implicit question regarding the role of the regulator, and the extent to which it is able to supervise institutions equally.
(iv) The concern is that wording in paragraph 52 will give credence to the de-risking phenomenon that is creating an unbanked remittance sector. This will result in adverse competitive factors and may ultimately result in the displacement of payments to the unregulated sector.

We urge the EBA to remove the last sentence of paragraph 52, and to replace it with a sentence clarifying the demarcation of responsibilities in relation to domestic firms. It is important for the EBA to help reinforce the compliance boundaries of banks, in order for banks to be able to manage their risk effectively, and enter into relationships with other PSPs without regarding this as an unquantifiable source of risk.

60 Other considerations

This provision is helpful. We suggest that the language is made more specific, by clearly describing the harm that is being addressed, the need for a case by case risk assessment, and the need to maintain banking services for other financial institutions and payment service providers.

We would also like to draw attention to the UK FCA statement on this matter, which goes further and sets out outcome expectations as well as general principles. It states:

"Firms should note that the application of a risk-based approach does not require them to refuse, or terminate, business relationships with entire categories of customers that they associate with higher ML/TF risk, as the risk associated with individual business relationship will vary, even within one category. ***While the decision to accept or maintain a business relationship is ultimately a commercial one for the bank, there should be relatively few cases where it is necessary to decline business relationships solely because of anti-money laundering***

requirements. As a result, supervisors should, when supervising AML compliance, should consider whether firms' de-risking strategies give rise to consumer protection and/or competition issues."

It is also helpful to be more specific and address the offer of banking facilities to other payment service providers in particular. The provisions of the second Payment Services Directive which requires credit institutions to provide reasons for refusing to extend such facilities to other payment service providers is helpful in this regard and can be referenced. This has the effect of creating a default position of enabling access to banking services, and EBA guidance can therefore go further. It can reference the obligation under PSD2 and clarify that the risk assessment should relate to the client payment service provider itself and not extend to the client's customers.

2. **Do you consider that these guidelines are conducive to competent authorities effectively monitoring firms' compliance with applicable AML/CFT requirements in relation to individual risk assessments and the application of both simplified and enhanced customer due diligence measures?**

Yes, subject to comments we have made in relation to both general guidelines (above) and sector specific guidelines (below).

3. **The guidelines in Title III of this consultation paper are organised by types of business. Respondents to this consultation paper are invited to express their views on whether such an approach gives sufficient clarity on the scope of application of the AMLD to the various entities subject to its requirements or whether it would be preferable to follow a legally-driven classification of the various sectors; for example, for the asset management sector, this would mean referring to entities covered by Directive 2009/65/EC and Directive 2011/61/EU and for the individual portfolio management or investment advice activities, or entities providing other investment services or activities, to entities covered by Directive 2014/65/EU.**

We support the structure of the guidelines and have a number of specific points to raise in relation to the e-money sectoral guidelines. These are set out in the table below.

Para	Provision	Comments	Remedy
111	The degree of ML/TF risk associated with electronic money (E-money) depends primarily on the features of individual E-money products and the degree to which E-money issuers use other persons to distribute and redeem E-money on their behalf.	This is unlike the introductions in the other sections, which set out how that particular sector/product type might be used for AML or TF purposes. The factors indicating risk should be set out in the paragraphs below, rather than in the introduction. It is an overstatement that the risk associated with e-money is dependent on the degree to which third parties distribute e-money.	We would welcome more information regarding how e-money products might be used for AML/TF purposes, rather than references to risk factors. It would be preferable to state that the more complex the value chain the greater the attention that needs to be given to risks arising from the outsourcing of different functions.
114, first bullet point, ii	… allows high or unlimited number of payments, loading or redemption, including cash withdrawal;	This provision would benefit from additional clarity, as the text does not provide a timeframe for such transactions. There is no reason to believe that a high or unlimited number of payments alone presents a risk of money laundering. This factor should not refer to the number of payments.	"allows high ***value*** ~~***or unlimited number of payments,***~~ loading or redemption, including cash withdrawal"
114, second bullet point, i	… can be loaded anonymously, for example with cash, anonymous E-money or E-money products that benefit from the exemption in Article 12 of Directive (EU) 2015/849	The reference to 'anonymous e-money' is not needed. E-money issued under the Art. 12 exemption is sufficient. According to these guidelines, all other e-money will involve at least the identification of the customer.	"can be loaded anonymously, for example with cash, ~~***anonymous E-money***~~ or Emoney products that benefit from the exemption in Article 12 of Directive (EU) 2015/849;"

114, second bullet point, ii	… can be funded with payments from unidentified third parties.	This raises a number of issues: 1) Almost all payment products can be funded by unidentified third parties, so it is difficult to support this provision. A bank account funding a transaction for example could previously have been funded from an anonymous cash deposit into the account. It is not clear that third party funding gives rise to any additional risk where cash funding is permissible. 2) It is not always possible for the issuer to detect this so the provision is impractical. 3) For anonymous products, a payment from a third party whom the issuer knows to have been identified by its payment service provider would have no impact on the money laundering risk.	Delete
114, third bullet point, ii	… is accepted as a means of payment by a large number of merchants or points of sale;	The number of merchants is usually dependent on the card scheme involved and is not indicative of risk. Transactions will involve the purchase of goods or services. Including this factor seems to suggest that a product's AML risk increases the more successful it becomes.	Delete

114, third bullet point, iv	… can be used in cross-border transactions or in different jurisdictions;	The nature of e-commerce makes this an unreasonable factor. Risk should be focused on the precise location where the e-money instrument can be used rather than on the ability to carry out cross-border transactions in itself.	Can be used in ~~***cross-border***~~ transactions ***to*** ~~***or in different***~~ jurisdictions ***categorized as high risk***;
114, third bullet point, v	is designed to be used by persons other than the customer, for example certain partner card products;	This provision could be regarded as capturing gift cards which re usually transferred to other person; and which are usually below 4MLD exemption thresholds. They do not usually give rise to higher risks.	is designed to be used by persons other than the customer, for example certain partner card products, ***but not low value gift cards***;
114, third bullet point, vi	… allows cash withdrawals.	Small cash withdrawals do not constitute a money laundering risk and may be necessary for customers to redeem remaining balances. This factor would be better expressed to take account of the value of cash withdrawals. Cash withdrawal below the 4MLD EUR 100 threshold for example are low risk.	allows ***high value*** cash withdrawals.
115 First bullet (ii)	limits number of payments, loading or redemption, including cash withdrawal in a given period;	Limiting the number of payments is better not featured as a factor indicating lower risk. There are many legitimate reasons for frequent payments.	Delete reference to frequent payments

115 Second bullet (i)	Requires that the funds for purchase or reloading are drawn from an account held in the customer´s name at an EEA credit or financial institution;	Establishing the name in which an account is held is in most cases impossible. It is however possible to establish who has control over the account and access to it. This acts as a reasonable proxy, and is the approach taken by issuers. Allowing for the establishing of control over the account would enable an equivalent or greater degree of certainty to be established.	Add at the end of the sentence**…'or one over which the customer can be shown to have control'**
115, third bullet point, ii and corollary 114 third bullet (iv)	114: can be used in cross-border transactions or in different jurisdictions 115: can only be used domestically;	It is too general to stipulate that cross border use of a product gives rise to higher risk, and the converse. A three party scheme may have users located in different member states or outside the EU transacting in accordance with set risk criteria, and where all transactions are visible. Four party systems may also operate within set common risk criteria on a cross border basis.	(i) Add: can be used in cross-border transactions or in different jurisdictions **"where such jurisdictions give rise to greater risk."** (ii) Delete reference in 115 to lower risk where use is only domestic.

115, third bullet point, iii	… is accepted by a limited number of merchants or points of sale whose business the E-money issuer is familiar with;	In conjunction with the higher risk factor under 114, third bullet point, ii above, this factor would effectively mean that all scheme-enabled cards (which are not accepted by a "limited" number of merchants or points of sale) need to be classed as higher risk. Widespread acceptance is too general a factor. Payment schemes require standardized CDD processes for their acquirers and provide merchant category codes to give issuers some general information. Complete absence of knowledge is unlikely to arise, and therefore the risk in relation to these cards should not be regarded as high.	Delete Paragraph 114, third bullet point, ii

116, first bullet point	… the customer purchases several E-money products from the same issuer or frequently reloads the product, or makes several cash withdrawals, in a short period of time and without economic reasons; where distributors are obliged entities themselves, this also applies to E-money products from different issuers;	Distributors have no systems of their own to either track users of a single issuer, nor across multiple issuers. The behavior of users of a single payment product is visible to the issuer, and distributors should not be obligated to duplicate systems that already exist. The risk of users opening multiple accounts with different issuers is addressed by the low values associated with exempted or SDD products. Once CDD is undertaken, the risk is no different to a user opening multiple bank accounts.	Delete references to the distributor monitoring multiple funding and redemption by users, whether singly or across multiple issuers. "the customer purchases several E-money products from the same issuer or frequently reloads the product, or makes several cash withdrawals, in a short period of time and without economic reasons, ~~**where distributors are obliged entities themselves, this also applies to E-money products from different issuers,**~~ ***and/or in a manner which is inconsistent with the product usage expected by the issuer."***
116, third bullet point	… the product appears to be used by several people whose identity is not known to the issuer (e.g. the product is used from several IP addresses at the same time);	Several IP addresses connected to one account do not necessarily mean that several people are using the product. The example would however be unusual, but not always suspicious: for example a corporate expense card can be used to make purchases by a number of staff at the same time.	the product appears to be used by several people whose identity is not known to the issuer ~~**(e.g. the product is used**~~ from several IP addresses at the same time~~**)**~~;

117	… The product is available only to certain categories of customers, e.g. social benefit recipients.	This is the only customer-related lower risk factor and thus appears to suggest that only corporate or public authority products offer lower customer risk. We suggest adding additional categories such as: • Employee gift card schemes • Payroll products – aimed at corporates to pay their own employees. • Incentive / commission – either corporate (aimed at particular types of individuals who undertake activity for a corporate (e.g. surveys) or consumer (for purchasing a product from a corporate) • Other incentive/reward products that can only be loaded by a company Provided that in all cases the corporate or similar entity has been subject to appropriate CDD	The product is available only to certain categories of customers, e.g. social benefit recipients, ***or incentive, reward, payroll, corporate expense or similar product that can only be loaded by a company or similar entity that has been subject to adequate CDD measures.***
118, first bullet point	… online and non-face to face distribution without adequate safeguards;	What are 'adequate safeguards'? Why would purchase of an e-money instrument in a supermarket constitute less risk than purchase of it online?	Delete or provide further clarification regarding what "adequate safeguards" might be.

122, last bullet point	… establishing the source and /or the destination of funds.	It is not clear what this refers to that goes beyond the measures already listed in the first and fourth bullet points.	Delete.
124, second bullet point	… verifying the customer´s identity on the basis of a payment drawn on an account in the sole or joint name of the customer with a EEA-regulated credit institution;	This should be re-phrased to focus on the control of the customer over the payment account, as e-money issuers are usually unable to verify the name on the funding account. They can however establish if the customer has control over the account, which provides assurance that the person using the account is the account holder or someone with right of access to it.	"verifying the customer´s identity on the basis of a payment drawn on an account ~~***in the sole or joint name of the customer***~~ with a EEA-regulated credit institution ***over which the customer can be demonstrated to have control***;"
124, sixth bullet point	… assuming the nature and intended purpose of the business relationship where this is obvious, e.g. certain gift cards that do not fall under the closed loop/closed network exemption;	Whilst helpful, it could be read to suggest that for more general purpose products, the nature and intended purpose of the business relationship cannot be assumed and may have to be individually ascertained.	Suggest adding: "***or other products that serve a particular purpose***"

124, last bullet point	… reducing the intensity of monitoring as long as a certain monetary threshold is not reached. As ongoing monitoring is an important means of obtaining more information on customer risk factors (see above) during the course of a customer relationship, that threshold should not exceed EUR 250 for individual transactions or transactions that appear to be linked over the course of 12 months.	The implication of including this threshold is that low risk cannot be present beyond EUR 250.	reducing the intensity of monitoring as long as a certain monetary threshold ***that can be demonstrated to be low risk*** is not reached. ~~***As ongoing monitoring is an important means of obtaining more information on customer risk factors (see above) during the course of a customer relationship, that threshold should not exceed EUR 250 for individual transactions or transactions that appear to be linked over the course of 12 months.***~~

List of EMA members as of January 2016:

- 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
- 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
- MarqMillions
- One Money Mail Ltd
- Optimal Payments
- Park Card Services Limited
- Payleven Ltd
- Payoneer
- PayPal Europe Ltd
- PayPoint Plc
- PPRO Financial Ltd
- Prepaid Services Company Ltd
- PrePay Technologies Ltd
- PSI-Pay Ltd
- QMoney
- R. Raphael & Sons plc
- Securiclick Limited
- Skrill Limited
- Stripe
- Syspay Ltd
- Transact Payments Limited
- TransferWise Ltd
- Valitor
- Wave Crest Holdings Ltd
- Wirecard AG
- Worldpay UK Limited
- Yandex.Money