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

Piers Haben
European Banking Authority
Floor 46,
1 Canada Square,
London E14 5AA

24 September 2018

Dear Piers,

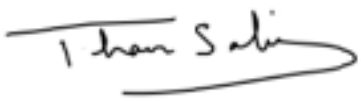
Re: EMA Consultation Response to Draft EBA Guidelines on outsourcing arrangements

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 on the draft Guidelines.

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

Yours sincerely,



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

EBA Consultation Questions:

Q1: Are the guidelines regarding the subject matter, scope, including the application of the guidelines to electronic money institutions and payment institutions, definitions and implementation appropriate and sufficiently clear?

Overall, the Electronic Money Association (EMA) find that the Guidelines identify the requirements that apply to outsourcing arrangements established by financial institutions in a clear manner.

We would request that the EBA provide more clarity on the *Date of Application* and the *Transitional Provisions* detailed in Paragraphs 12/13 of the Consultation paper ("CP"). Specifically, the time afforded to financial institutions to align their outsourcing arrangements for Critical/ Important functions with the requirements in these GLs. Here, we note the date of 31 December 2020 (that appears in par.13) only refers to documenting such outsourcing arrangements rather than ensuring compliance with other requirements in these GLs (due diligence, risk assessment, oversight, exercise right of audit etc.)

We would also request that the definition of outsourcing in the Table in par. 11 of the CP is expanded to include some clearer examples of services delivered to an institution that are considered outsourcing.

Q2: Are the guidelines regarding Title I appropriate and sufficiently clear?

The Guidelines regarding Title I are clear.

Q3: Are the guidelines the guidelines in Title II and, in particular, the safeguards ensuring that competent authorities are able to effectively supervise activities and services of institutions and payment institutions that require authorisation or registration (i.e. the activities listed in Annex I of Directive 2013/36/EU and the payment services listed in Annex I of Directive (EU) 2366/2015) appropriate and sufficiently clear or should additional safeguards be introduced?

We would welcome additional clarity on the following areas:

1. The full scope of acquired services "*not normally performed by the institutions*" that are not considered outsourcing. The examples provided in Par.23 are rather limited. For example, are the services provided by utilities (water, electricity, telecoms/IP) considered outsourcing? Is the delivery of regulated payment services from an authorised 3rd party (banking services provider, payment card transaction acquire, merchant acquirer) to be considered outsourcing? Here, we would encourage the EBA to align the examples of services that are not considered outsourcing with the Definition of outsourcing in the Table in Par.11[1].
2. Do all conditions - detailed in Par. 26 – need to be met for an institution to outsource banking activities or payment services to an outsourcer located in a non-Member state?
3. How can institutions confirm the existence (and scope of coverage) of an MoU between competent authorities as detailed in Par. 26(c)? Here, we propose that the EBA (or national CAs) publish and maintain a list of 3rd party jurisdictions that would satisfy the supervision authority co-operation requirements detailed in this Paragraph.

Q4: Are the guidelines in Section 4 regarding the outsourcing policy appropriate and sufficiently clear?

The EMA are concerned by the overly prescriptive approach adopted by the EBA to identifying the contents of the Outsourcing Policy. We believe that institutions should be afforded some flexibility in drafting this Policy.

We consider that the explicit requirement to document an Exit Plan for every Critical/Important outsourced function will require a significant effort investment on the part of the institutions with limited returns. Additionally, the operational advantages that the current requirement delivers to financial institutions are already addressed by the institutions' business continuity arrangements.

Section 10.4 of these Guidelines (par. 82) also includes guidance on setting an appropriate transition period in any outsourcing agreement to migrate away from an outsourcer. Therefore, we would propose that the requirement to document an Exit Plan for every Critical or Important function is deleted.

---

[1] Please see our response to Question 1 of the Consultation, above.

The EBA's rationale behind the requirement to differentiate between outsourcers that are authorised by a competent authority and those that are not authorized is unclear.

Q5: Are the guidelines in Sections 5-7 of Title III appropriate and sufficiently clear?

We are concerned that the requirement to have the outsourcing institution's internal audit function ascertain an outsourcer's "*risk appetite, risk management and control procedure are in line with the institution's strategy*"[2] will be very difficult to achieve in many instances. Global outsourcers are unlikely to be prepared to share insights on the outcomes of their internal risk management process with most of their clients.

Q6: Are the guidelines in Section 8 regarding the documentation requirements appropriate and sufficiently clear?

The EMA are concerned by the overly prescriptive approach adopted by the EBA to identifying the contents of the *Register of outsourcing arrangements*. We believe that institutions should be afforded some flexibility in drafting this Register especially for non-Critical or Important functions.

We seek more clarity on the EBA rationale in including cloud service providers to the list of outsourcers covered by the register detail listed in Par. 47(c). A number of cloud-based outsourced services may not involve Critical or Important functions of the institution; in such an instance, we are not clear why a risk-based supervisory approach would require outsourcing institutions to provide additional information for such service providers.

We question the value-add delivered by the requirement to identify alternative service providers and to list the estimated annual budget cost of an outsourcing relationship in the Register, as detailed in Par. 47(c)vii and 47(c)x, respectively. The latter is also likely to be commercially sensitive information that should not interest the competent authority.

Q7: Are the guidelines in Section 9.1 regarding the assessment of criticality or importance of functions appropriate and sufficiently clear?

[2] See Par. 44(d)

We invite the EBA to clarify the statement in Par. 51 (a) that identifies an outsourcing arrangement to be critical or important where it is "*directly connected to the provision…*" of the authorized services. The existing statement is open to multiple different interpretations; as such, it may be useful to consider deleting this text altogether. The existing text at the start of Par.51 already identifies Critical or Important arrangements as those that deliver Critical or Important Functions; these functions are already identified by an institution's Business Impact Analysis (BIA).

Q8: Are the guidelines in Section 9.2 regarding the due diligence process appropriate and sufficiently clear?

The text in Par.56 includes a high-level reference to an outsourcing institution's "*values and code of conduct*" and a requirement for the institution to be satisfied that all outsourcers adhere to international standards on human rights, environmental protection and appropriate working conditions. The EMA expect that many outsourcing institutions will find it very difficult to confirm that the working policies and values of global outsourcers fully align with the institutions' code of conduct across all service locations. We are also not clear how outsourcing institutions should treat differences on such standards (and applicable local legislation) across different jurisdictions.

We would welcome more guidance from the EBA on how outsourcing institutions can satisfy this requirement in practical terms.

Q9: Are the guidelines in Section 9.3 regarding the risk assessment appropriate and sufficiently clear?

We find the reference to a specific risk mitigation control (use of encryption) that appears in Par. 61 (e) to be out of place with the remaining content of Section 9.3. Institutions may choose to use a range of risk mitigation controls to address risks identified during the outsourcer risk assessment detailed in this Section; we see no reason that only one such control is identified explicitly at the end of this Section. We propose that the references to encryption are removed from the end of Section 9.3.

Q10: Are the guidelines in Section 10 regarding the contractual phase appropriate and sufficiently clear; do the proposals relating to the exercise of access and audit rights give rise to any potential significant legal or practical challenges for institutions and payment institutions?

We are concerned that the Guidelines detailed in Section 10 will create significant practical challenges for many institutions if they are adopted in their current form. Specifically:

1. The requirement that a written outsourcing agreement identifies all data storage/processing locations and includes a requirement that the outsourcer notifies the institution of proposed changes in these locations (see Par. 63 (e)) may be very difficult to meet by institutions that use cloud-based service providers. Such providers often assign data processing resources on a dynamic basis making use of available network capacity and resource availability; as such, it would be very difficult to ask them to provide a notification of change every time that a new data processing resource (hosted in a different virtual location) is used.

2. Par 63(h) and Par 72(b) put forward a requirement that outsourcing institutions should insist that they are afforded an *unrestricted* right of access and audit with respect to an outsourced service. This requirement appears to ignore current market dynamics whereby global outsourcers support thousands of outsourcing institutions using multiple locations. The expectation that any large outsourcer will agree to unrestricted access/audit rights to clients is not realistic. Instead, we propose that the required right of access/audit is framed more closely around the delivery of the outsourced service as outlined in the rest of Section 10.3 We propose that the references to unrestricted rights of audit/access are also removed from Paragraphs 63(h) and Par 72(b).

3. The EBA rationale for the last sentence of Par. 74 ("*However, they should note rely solely on those*") is unclear. An outsourcing institution should be able to rely on the use of 3rd party certifications and audit reports to meet the requirements in Section 10 if the institution is comfortable with the expertise/independence of the auditor and suitability of the audit framework that is used to carry out these audits. We propose that this sentence is removed from Par.74.

4. Par 81(b) proposes that the outsourcing institution retains the right to terminate an outsourcing agreement if it identifies impediments capable of altering the performance of the outsourced service. This is a termination condition that appears to be based not on observed

outsourcer service delivery performance; rather, an assessment of future performance is made by the institution. As such, we believe that it will be practically very difficult to convince outsourcers to accept such a termination condition. Additionally, text in Par 81(c) already covers "*material changes affecting an outsourcing arrangement*". We propose that the text in Par. 81(b) is removed.

Q11: Are the guidelines in Section 11 regarding the oversight on outsourcing arrangements appropriate and sufficiently clear?

The guidelines in Section 11 are clear.

Q12: Are the guidelines in Section 12 regarding exit strategies appropriate and sufficiently clear?

We are concerned that the Guidelines in Section 12 introduce unnecessary additional work for outsourcing institutions. Specifically:

1. The requirement to develop, ***implement and test*** an Exit Plan for all outsourced Critical or Important functions (Par. 90 (a)) will deliver limited additional benefits to outsourcing institutions. These institutions are already required to produce and test Business Continuity Plans (BCPs) that address the continued delivery of regulated services in case of unavailability/lack of performance by major outsourcers. We propose that the requirement to implement and test an Exit Plan for all outsourced Critical or Important functions is removed.
2. The additional benefits delivered by the requirement to complete a BIA for Critical/ Important outsourced functions (Par. 91(b)) are limited; outsourcing institutions are already expected to identify the resources/activities required to switch an outsourcing relationship in the course of developing an Exit Plan for such a relationship. We propose that the text in Par 91(b) is removed.

Q13: Are the guidelines in Section 13 appropriate and sufficiently clear, in particular, are there any ways of limiting the information in the register which institutions and payment institutions are required to provide to competent authorities to make it more proportionate and, relevant? With a

view to bringing sufficient proportionality, the EBA will consider the supervisory relevance and value of a register covering all outsourcing arrangements within each SREP cycle or at least every 3 years in regard of the operational and administrative burden?

The EMA seek further clarity on the frequency of submission of the Register of all existing outsourcing arrangements to competent authorities. Additionally, we encourage the EBA to work with EU/EEA national competent authorities to establish a consistent reporting frequency/format across all authorities. This would allow outsourcing institutions that are present in multiple EEA jurisdictions to harmonise their reporting processes.

Furthermore, we believe that the requirement that institutions should inform competent authorities of outsourcer events that have a material impact on the delivery of a regulated service (Par. 95) duplicates existing requirements detailed in the *EBA Guidelines on Major Incident reporting* (EBA-GL-2017-10). We propose that Par.95 is removed.

Q14: Are the guidelines for competent authorities in Title V appropriate and sufficiently clear?

The Guidelines in Title V – aimed at competent authorities – are clear.

We would like to highlight that competent authorities are very likely to identify concentration risks in the provision of cloud-based outsourced hosting services. The industry is dominated by a few large players (AWS, MS Azure, Google Cloud etc.) that leverage economies of scale to deliver services at price points that are difficult to match by smaller players. It is not clear how competent authorities will address evidence of such concentration risks at sectoral level.

Q15: Is the template in Annex I appropriate and sufficiently clear?

We find the template in Annex I to be rather complicated. Additionally:

1. We would propose that References to *Estimated Budget cost* (cell S5) and *Examples of Alternative Service Providers* (cell AA5) in the *Submission of Information* tab are removed from the Template for reasons highlighted in our response to Q.6, above.
2. The list of *ICT Activities* identified in the *List of Activities* tab is quite limited and should be expanded to cover more of the ICT activities that are outsourced by institutions (software

development/testing/ deployment/maintenance, hardware deployment/maintenance, IP communications, telecoms networks, IT security, network maintenance, device management etc.)

Q16: Are the findings and conclusions of the impact assessments appropriate and correct; where you would see additional burden, in particular financial costs, please provide a description of the burden and to the extent possible an estimate of the cost to implement the guidelines, differentiating one-off and ongoing costs and the cost drivers (e.g. human resources, IT, administrative costs, etc.)?

We have a number of concerns on the Impact Assessments detailed in Section 5.1. These are:

1. Impact Assessment 5 underestimates the additional overheads that outsourcing institutions will have to carry to maintain a Register for all outsourcing arrangements rather than just for outsourced Critical or Important functions (Option B2). Such overheads comprise human and administrative costs. We would also expect the recipients of Register information (competent authorities) to incur additional costs in processing submitted Register information. Instead, Option B1 would deliver the necessary information on Critical outsourcing arrangements to competent authorities without the additional "clutter" of non-Critical outsourcing arrangements.
2. Impact Assessment 7 (outsourcing of banking activities) resulted in retaining Option A even though it places additional restrictions on the choice of banking/payment services' outsourcers based on the existence of Co-operation Agreements between CAs. It is difficult to understand the rationale behind the choice of Policy Option A when the impact assessment acknowledges the length of negotiations between CAs to establish such co-operation agreements and the limiting effect that the time to conclude such negotiations may have on the outsourcing policy of financial institutions.

List of EMA members as of September 2018:

Airbnb Inc
Allegro Group
American Express
Azimo Limited
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network Ltd
Boku Inc
CashFlows
Circle
Citadel Commerce UK Ltd
Coinbase
Corner Banca SA
Curve
Ebanx
eBay 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
Ozan
Park Card Services Limited
Paybase Limited
Payoneer
PayPal Europe Ltd
PayPoint Plc
Paysafe Group
PPRO Financial Ltd
PrePay Solutions
QIX Ltd
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
TrueLayer Limited
Trustly Group AB
Uber BV
Valitor
Vitesse PSP Ltd
Viva Payments SA
Wave Crest Holdings Ltd
Wirecard AG
Wirex Limited
Worldpay UK Limited