State Street Corporation

20 Churchill Place
Canary Wharf
London E14 5HJ

T +44 20 3395 2500
F +44 20 3395 6350

www.statestreet.com

24 September 2018

European Banking Authority

Via electronic submission

Dear Sir/Madam,

EBA Consultation: Draft Guidelines on Outsourcing Arrangements

State Street Corporation appreciates the opportunity to comment on the EBA's consultation on the draft guidelines on outsourcing arrangements.

State Street Corporation (NYSE: STT) is one of the world's leading providers of financial services to institutional investors, including investment servicing, investment management and investment research and trading. With $33.90 trillion in assets under custody and administration and $2.70 trillion[1] in assets under management as of June 30, 2018, State Street operates in more than 100 geographic markets worldwide, including the US, Canada, Europe, the Middle East and Asia. For more information, visit State Street's website at www.statestreet.com.

State Street welcomes the publication of the draft guidelines and recognises the importance of effective internal governance arrangements over outsourcing. However, we believe there are a number of areas where the guidelines could be further developed and more clearly reflect the principle of proportionality.

As an overarching observation, it strikes us that although framed as "guidelines", the proposed text is highly prescriptive. It may be helpful if the drafting could differentiate between regulatory requirements (which are mandatory) and guidance (which allows for flexible and proportionate application). We have set out below some issues which reflect this theme in the interest of allowing institutions to align the risk of each outsourcing arrangement with the associated compliance cost.

In addition to using a measure of proportionality on outsourcing arrangements, we believe it is important to make the draft guidelines more applicable by allowing minor differences between internal and external outsourcing arrangements. There are implications to a financial institution for collection of financial information at detailed

[1] Assets under management include the assets of the SPDR® Gold ETF and the SPDR® Long Dollar Gold Trust ETF (approximately $33 billion as of June 30, 2018), for which State Street Global Advisors Funds Distributors, LLC (SSGA FD) serves as marketing agent; SSGA FD and State Street Global Advisors are affiliated.

levels for internal providers, covered by step-in rights, as well as the level of recertification required if the internal provider is part of global governance and oversight practices.

Whilst we recognise the need for safeguards to ensure Member State competent authorities can effectively supervise third country outsourcing arrangements of regulated entities, we do not believe that it would be workable for the onus to be placed on institutions to ensure that an appropriate cooperation agreement is in place between their own supervisory authority and the service provider's supervisory authority. We believe the better approach would be for each local supervisory authority to maintain and issue a list of countries to which outsourcing is appropriate, rather than for each institution making its own determination as to where the relevant authorities may stand relative to each other and the specific provisions of their agreements.

Finally, we are concerned that the draft guidelines are likely to place requirements on firms to source information from IT providers or other third parties located in jurisdictions whose national law prevents firms from having a right to access such information, and thus leaving them unable to fulfil their obligations under the guidelines. This is of particular concern where a niche service is being provided or if there is only small number of specialised providers available. We would therefore recommend the inclusion of an exception mechanism in close cooperation with relevant national competent authorities, which would allow the use of such third party providers in such specific situations.

Thank you for the opportunity to comment on the important matters raised within this discussion paper. Please feel free to contact us should you wish to discuss State Street's submission in greater detail.

Sincerely,

Elspeth Todd.

Elspeth Todd
Senior Vice President
Head of Outsourcing EMEA

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?

In relation to the proposed definition of outsourcing in paragraph 11, consideration should be given to permitting institutions to self-identify their own excluded activities based on criticality and proportionality.

In reference to the definition of a critical or important function, the guidelines state that the definition includes "*any operational tasks performed by the internal control functions*". However, it is important to note that internal control functions perform a range of tasks some of which have a bearing on the institution's risk profile and others which do not (e.g. routine administrative tasks). Therefore, we believe it should be up to the institution to determine whether the particular task being outsourced is in fact "*critical or important*". Also, in addition to the criteria laid out in section 9.1 of the guidelines, we would welcome the use of examples to further help firms identify critical or important functions as otherwise there is a risk that different firms will interpret the guidelines differently and have significantly different approaches to implementation.

We would welcome clarification on what priority firms should apply to the requirements under MIFID II and BRRD in reference to recovery and resolution planning, resolvability and operational continuity. We understand from the draft guidelines that, as suggested in paragraph 50, the definition in MiFID II would generally be applicable when determining whether a function is critical or important. However, paragraph 51 contains a reference to recovery and resolution planning, resolvability and operational continuity. We would welcome clarification whether this means that in a recovery and resolution scenario a firm must take into account the definition in both the BRRD and MiFID II or only in the BRRD.

Lastly, the guidelines contain multiple use of the term '*location*' and we would welcome clarification that references to 'location' mean the country level.

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

We note that in the proposed guidelines, no proportionality based on risk profile is afforded to intra-group outsourcing. In our view, this does not recognize the degree of integration reached within many banking groups, where centralized functions at group level act as a service provider for the other entities of the group. For example, a number of the proposed requirements such as those relating to due diligence, concentration risk and exit strategies are not directly relevant to groups with intra-group outsourcing arrangements and as such we believe that intra-group outsourcing should be subject to calibrated requirements for due diligence and exit strategies. Similarly, we believe that proportionality based on a risk-based approach should be applied to the provision of corporate functions by parent organizations.

In relation to paragraph 20(b), and the ability for institutions in groups with a centralized outsourcing function to delegate the pre-outsourcing assessment in appropriate cases, we believe the requirement for each institution to receive the assessment at the time of outsourcing should only apply to the outsourcing of critical or important functions or

arrangements. All assessments could be provided on a regular basis for information as part of the financial institution governance.

Q3: Are 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?

Paragraph 26(b) places the onus on institutions to ensure that an appropriate cooperation agreement is in place between their own supervisory authority and the service provider's supervisory authority. We believe it would be more efficient for each local supervisory authority to issue a list of countries to which outsourcing is, or is not, appropriate, rather than for each institution to undertake its own assessment.

Further to this, standard market practice in the financial industry involves providing services to clients in the EU27 and certain activities are outsourced to affiliates, including affiliates operating in third countries. Therefore industry participants will be dependent on cooperation agreements being put in place between competent authorities otherwise firms, as well as the wider financial services industry in addition to end consumers across Europe, could face significant disruption and additional costs. Instead of requiring Memorandums of Understanding (MoUs) between Competent Authorities we advocate the adoption of an outcomes focused approach which would allow for more flexibility and which would not make the ability to outsource dependent on MoUs over which institutions have no control.

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

No comments.

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

In relation to Business Continuity Plans, we believe the proposed requirement in paragraph 40 to involve a service provider in testing where the failure to provide a critical or important function would lead to severe business disruption. It further would potentially have significant impact on providers, especially if they are external. It is therefore important that the final guidelines are clear on the expected level of involvement between the provider and client in such a process. We would recommend giving consideration to reliance on continuity testing done by a service provider for a service where results can be shared across multiple financial institutions. This reduces the burden on the providers for continuity testing to meet these guidelines for every individual institution.

We would welcome clarification of the wording in paragraphs 43 and 44 as it relates to the exercise and enforcement of audit rights. In our view, the current proposal could be interpreted to suggest that the corporate audit function is responsible for audit enforcement rights. We would therefore recommend clarifying that it is the outsourcing arrangement owners who should enforce audit rights to enable them to effectively oversee outsourced activities. Placing responsibility to enforce audit rights on the

corporate audit function would risk creating an inherent conflict of interest as the corporate audit function's mandate is to review the oversight arrangement controls and the structuring of oversight is the role of the first line of defence and not the third line.

In relation to paragraph 44(d), we believe the draft guidelines should make clear that the assessment of the service provider's risk appetite statement and control procedures should be assessed by the outsourcing arrangement owner as part of the risk assessment and continued oversight over the outsourced activity, rather than being the responsibility of the corporate audit function. The audit function has a role to ensure this is effective.

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

We are fully supportive of the need to maintain a register. However, we believe that firms should have the flexibility to maintain data that is substantially equivalent to that listed in the guidelines, but without having to meet all data points. The data points to be included in the outsourcing register are quite prescriptive, do not necessarily fully align with the current data points, and may not yield a significant benefit. In particular, data regarding sub-service providers should only be necessary for critical or important functions or functions in scope of GDPR due to the administrative burden it would place on firms to source this. We believe the most appropriate and proportionate approach would be for each institution to determine which data points should be captured having regard to the overall group structure, the criticality of each outsourcing arrangement, and relevant regulatory requirements.

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

With reference to paragraph 50, we believe not all processes or services relating to core business lines should be considered as "*critical or important*". A core business line may be comprised of numerous sub-processes, some of which will have little bearing on the institution's risk profile. As highlighted earlier, we believe it should ultimately be up to the institution to determine whether the function being outsourced is, in fact, "*critical or important*".

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

Paragraph 54 specifies the need to take into consideration additional factors such as the financial situation of a potential external service provider when conducting due diligence. However, we believe it is important to highlight that an institution may not always be able to gain access to the relevant financial information, esp. if it is not publicly available.

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

We believe the proposed requirements in paragraph 60 relating to sub-outsourcing should be linked to the materiality of the risk posed or whether it relates to a critical or important function.

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?

In reference to para 63(b), it should not be necessary for each outsourcing agreement to specify an end-date provided that appropriate termination provisions are included. We would also advocate that not all but only material changes to the outsourcing agreement would require to be expressly approved by the financial institution's responsible person or relevant legal entity board.

In relation to para 63(h), 66(b) and 72, the requirement for "*unrestricted*" or "*complete*" access and audit rights is not realistic. Such rights need to be balanced against the need for each service provider to manage issues of confidentiality, privacy, conflicts of interest, and business disruption that accompany audits and information requests. The service provider should be required to cooperate with requests from supervisory authorities and to grant appropriate audit and access rights with regard to the criticality of the function being outsourced. Additionally, it should not be necessary for the institution to have direct rights of audit and access to sub-outsourcing service providers provided that the original service provider carries out appropriate monitoring and oversight and gives appropriate contractual warranties to the service recipient institution.

As a general point on section 10, we wish to emphasise that the requirements on sub-outsourcing will be impossible for institutions to implement unless the competent authority has authority over these vendors since the firms themselves cannot require sub-outsourcers, particularly those which are IT related, to allow them oversight of their activities.

In reference to section 10.3 as it relates to the use of auditors and pooled auditors, we suggest there is a need for clarification as to whose auditors these would be in the context of intra-group outsourcing arrangements; for example would it be sufficient to use auditors from the wider group? We would also welcome clarification as to whether arrangements for the use of pooled auditors only relevant to external outsourcing arrangements? As highlighted earlier, we believe the draft guidelines should clarify that the enforcement of audit rights is that of the outsourcing arrangement owner and not that of the corporate audit function.

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

As highlighted earlier, we believe the proposed requirement for firms to be able to have oversight of sub-contractors as they relate to IT sub-contractors is unrealistic, given that there are no legal requirements on IT sub-contractors to allow firms oversight, and bears no relation to materiality, criticality/importance or risk.

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

The requirements in section 12 on exit strategies should reflect whether an outsourcing arrangement is with an intra-group or external provider and also be calibrated on risk

posed to the institution from a failure of the specific service provider or a material deterioration in the service provided.

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 bring 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.

We support the guidance to make available the full register of outsourcing arrangements to the competent authority. However, in relation to paragraph 92, we consider that in absence of a request, it would be more proportionate for institutions to provide the competent authority with only a subset of that register, consisting of critical or important outsourced functions.

In relation to paragraph 93, we do not consider that all of the information in paragraphs 47(a), (b) and (c) is of value to a competent authority and therefore it should be open to an institution's supervisors to determine what they would like to see.

Further to this, and as highlighted early, we believe some of the proposed requirements for the register would necessitate firms that have intra-group outsourcing arrangements to collect data that would not have a bearing on an outsourcing assessment of internal providers and collecting this would pose a significant unnecessary burden.

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

No comments.

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

No comments.

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 believe the conclusions of the impact assessments do not reflect the additional burden resulting from the increased scope of the guidelines on sub-outsourcing as well as their implications for current IT outsourcing arrangements.

We believe an important way of limiting undue burden and expense for firms would be to allow for calibration of the documentation requirements to be based on the criticality of provider and not just service.