4th floor
Ropemaker Place
25 Ropemaker Street
London
EC2Y 9LY
United Kingdom

tel +44 20 7260 2000
fax +44 20 7260 2001
www.markit.com

Financial Conduct Authority
25 North Colonnade
London E14 5HS
United Kingdom

Submitted via email to itoutsourcing@fca.org.uk

London, February 15th 2016

Proposed Guidance for firms outsourcing to the 'cloud' and other third-party IT services

Dear Sirs,

Markit is pleased to submit the following comments to the FCA in response to its *Proposed Guidance for firms outsourcing to the 'cloud' and other third-party IT services* (the "***Proposed Guidance***").

Markit[1] is a leading global diversified provider of financial information services.[2] Founded in 2003, we employ over 4,000 people in 11 countries and our shares are listed on Nasdaq (ticker: MRKT). Markit has been actively and constructively engaged in the debate about regulatory reform in financial markets, including topics such as the implementation of the G20 commitments for OTC derivatives and the design of a regulatory regime for benchmarks. Over the past years, we have submitted more than 140 comment letters to regulatory authorities around the world and have participated in numerous roundtables.

Introduction

Markit is a leading, established provider of innovative RegTech solutions with many of our services designed to support our customers' compliance with regulatory requirements across asset classes, throughout the trade workflow and for a range of financial market participants and service providers. Our RegTech services facilitate firms' compliance with regulatory requirements and reduce the related costs and risks, hereby lowering barriers to entry and fostering competition in the market place.

Markit is pleased to provide comments to the Proposed Guidance which, we hope, the FCA will find helpful in formulating its final guidance (the "***Guidance***"). We believe that the Proposed Guidance is very relevant for many firms and their service providers, including 'cloud' infrastructure providers, (***"Third Parties"***) given the substantial IT innovation that has occurred over the last several years. Markit appreciates these challenges and we believe we are well positioned to comment on the Proposed Guidance given our activities in the following areas:

[1] See www.markit.com for more details.
[2] We provide products and services that enhance transparency, reduce risk and improve operational efficiency of financial market activities. Our customers include banks, hedge funds, asset managers, central banks, regulators, auditors, fund administrators and insurance companies. By setting common standards and facilitating market participants' compliance with various regulatory requirements, many of our services help level the playing field between small and large firms and foster a competitive marketplace.

- **Outsourcing to cloud providers:** many of Markit's products and services are data intensive and we use a variety of methods to manage the relevant data in the most effective and efficient manner. Markit's applications and data are hosted internally in Markit data centers with a variety of third parties. The use, transfer and overall management of data is governed by a well-defined data classification definition. This definition identifies the differences between public, confidential and strictly confidential data among other sensitive data types. We follow industry best practice standards on security, confidentiality, as well as personally identifiable information (PII).[3] Furthermore, Markit's IT governance system ensures that data integrity and control standards that are applied to Markit's data centers would also be applied to our cloud providers.

- **Markit as a third-party IT service provider: w**e are also a leading third-party IT services provider and have gathered significant experience in managing the outsourcing needs of our clients, several of which are mentioned in the guidance letter.

- **Solutions to manage third-party risk:** Markit also provides specific solutions that assist our customers in managing their third party vendor risk.[4] These solutions take into account service providers in the supply chain and help firms to conduct due diligence on a multitude of third-party providers in an efficient manner.

Comments

We welcome the publication of the Proposed Guidance and we believe that the FCA's initiative in this area is timely given the challenges that firms face in relation to data security and privacy.

We welcome the FCA's stated aim to "avoid imposing inappropriate barriers to firms' ability to outsource to innovative and developing areas, while ensuring that risks are appropriately identified and managed".[5] We recommend the FCA ensure its proposals are consistent with its own RegTech initiative[6] which aims to foster the development and adoption of innovative services that facilitate firms' compliance with regulatory requirements. In this context, while we note that a number of recommendations made by the FCA in the Proposed Guidance in relation to data protection and security are constructive, it should not require firms to enact policies that result in discouraging their use of cloud and third party IT service providers. We believe that some elements of the Proposed Guidance could, in the extreme, cause firms to conclude that they can no longer use services of such third parties, which would be contrary to the aims of the FCA's own RegTech initiative.

To avoid such consequences we recommend the FCA make its Guidance more practical and not unnecessarily burdensome. Specifically, based on our experience as a third party IT service provider and user of cloud services we encourage the FCA to make the following changes in its Guidance:

- Many third parties are multinational companies with operations in a multitude of jurisdictions which allows them to offer the most efficient service to their clients; any obligations to notify their clients when opening a new business premise should only be required in cases where such action causes material change in their business relationship with its clients;

[3] In terms of outsourcing infrastructure to cloud providers, the specific controls within Markit relate to the sophisticated use of Virtual Private Cloud (VPC) implementations, hardened operating system images, network boundaries, host level security rules, integrated IAM (Identity and Access Management) implementations, reserved instances, data encryption services and use of VPN technologies.
[4] Markit's Know Your Third Party (KY3P) platform helps firms manage third party risk which includes due diligence and ongoing monitoring by providing a central data hub for centralising data on vendors and service providers. See http://www.markit.com/product/ky3p for details.
[5] Para 1.4, Pg 2
[6] https://www.fca.org.uk/news/call-for-input-regtech

- It should be the responsibility of third parties that their sub-contractor's comply with the guidelines and firms should not have the right to veto third parties' choice of sub-contractors;
- Centralised shared services can assist in mapping the supply chain and managing the risks contained in it in a transparent and auditable manner;
- Third-parties should be required to notify breaches only in cases of breach of NPPI;
- Third parties should have choice of jurisdiction in which they store, process and manage the data;
- Unrestricted access to data held by third parties would create excessive access, storage and control costs;
- Firms' visits to third party business premises should be limited and should only be conducted by qualified professionals;
- Subcontracting arrangements by third parties contain sensitive information and as such they should not be required to share them with firms;
- The FCA's proposals on resolution should be limited to cases where third parties provide critical outsourcing services to firms; and
- Third parties should only be expected to co-operate reasonably with other third parties and in a manner that protects the intellectual property rights in the event firms exit critical outsourcing services of the third party in question.

Legal and regulatory considerations

The guidance states that firms should "know which jurisdiction the service provider's business premises are located in and how that affects the firm's outsource arrangements"[7].

In this context, the FCA should consider that many third parties are big multinational companies that are opening new premises in different jurisdictions on an ongoing basis. The guidance should therefore not amount to requiring third parties to inform all its customers every time they expand into a new business premise. Third parties should be required to provide notifications to their clients only in the event that their expansion into new business premise results in a material change in the business relationship.

The FCA proposed that firms need to be in a position to identify "all the service providers in the supply chain and ensure that the requirements on the firm can be complied with throughout the supply chain"[8]. The FCA should note that it is generally the responsibility of third parties that provide services to regulated firms to ensure that other third parties on which they depend perform at the required level. It should hence be the right of third parties to choose their sub-contractors. To reflect practical realities we recommend the Guidance should be appended to specify that firms cannot veto the choice of sub-contractors used by third parties and those third parties should not be obliged to provide notifications to their clients when choosing their contractors.

We also believe that firms that have third party dependencies might often not be completely aware of the dependencies of their third party providers. Supply chains are often complex, which can result in challenges from a risk management and business continuity perspective. Our experience has shown that the use of centralized shared services[9] helps firms to manage their supply chain effectively, including mapping the supply chain and notifying firms of key events in the supply chain.

Risk management

[7] Pg. 8
[8] Pg. 8

The Proposed Guidance states that firms should require "prompt and appropriately detailed notification of any breaches or other relevant events arising including the invocation of business recovery arrangements" and "ensure the contract(s) provide for the remediation of breaches and other adverse events."[10]

The FCA should note that requiring third parties to notify the firms they are providing services to of each and every breach or "other relevant events" is likely to be very expensive for third parties without commensurate benefits. We therefore recommend that any requirements for the provision of notifications are limited to breaches that have a "material impact" on the business relationship or in the event of breaches in relation to NPPI.

Data security

The FCA stated that firms should have in place "a data residency policy that sets out where data can be stored".[11]

We believe that a data residency policy which is overly prescriptive and expects firms to require their third-party IT and cloud providers to store data within particular jurisdictions would lead to, for example, greater technological complexity and inconsistent requirements for logical and physical data separation. This, in turn, would result in greater operational, maintenance audit, reporting and regulatory overhead costs for such vendors which would be reflected in increased cost of service to the firms that use them.

When services being offered are either truly multi-tenant or data is shared or replicated between regions then implementing regional residency of data is technologically complex and costly. For example, regional data residency policies are compounded by the Joiner/Transfer/Leaver[12] process where clients of third parties are required to access data from different jurisdictions which would make it almost unrealistic to manage regional transfers in a consistent way. The FCA should be cognizant of the fact that a number of third parties provide services to firms domiciled in various jurisdictions. If firms' data residency policies required third parties to store data in each of these jurisdictions, it might result in these services no longer being viable. The FCA should note that third parties make large investments in managing data centers which will be subject to strict data security and privacy standards which should alleviate concerns of firms that are outsourcing to third parties in these cases.

However, when firms are offering enterprise level services which are delivered to a firm in a particular jurisdiction then it would be possible, and even beneficial, for third parties to conform to regional data residency clauses. This is because cloud providers support many regions, simplifying data storage and delivery within a particular jurisdiction.

The FCA should also note that, for data protection reasons, some of the major cloud providers do not actually reveal the location of their data centers to their users. Such common practice would make it very difficult for firms to "have choice and control regarding the jurisdiction in which their data is stored, processed and managed".[13] Irrespective of these concerns, we believe that it would be very challenging for third parties to store data in the choice of jurisdiction of their clients.[14] Also, focusing on the jurisdiction in which the data is stored does not resolve data security related issues since the data would still need to be managed and

[10] Pg. 9
[11] Pg. 10
[12] Joiners/transfers/leavers is a term used to describe the movement of staff to different offices across the globe.
[13] Pg. 10
[14] We note that some jurisdictions, e.g., Germany or Russia, have adopted regulations that require data owned by firms domiciled within their jurisdictions to be stored within the physical boundaries of the country. Such requirements have created significant costs for third parties that are offering services to these firms. We believe that this aspect of the FCA's Proposed Guidance creates a dangerous precedent as it puts the onus on third parties to defer to their clients on data location. We are concerned that it would actively incentivize firms to require their third parties to locate the data within their jurisdiction. As a result, third parties serving these firms would need to create data storage infrastructure in each jurisdiction their clients are based in which is likely to result in a massive increase in cost of the service and destroy a significant portion of the efficiencies that they currently generate.

processed from a remote location. If third parties are limited in their ability to process and manage data stored in other jurisdictions it would be impossible for them to discharge their duties effectively.

The Proposed Guidance also states that firms should "consider how data will be segregated (if using a public cloud)".[15] In this context, the FCA should consider that, by definition, public clouds are multi-tenanted data infrastructures which segregate data virtually for each of their users. We therefore recommend the FCA specify what exactly the firms should consider when employing the services of public cloud infrastructures.

Effective access to data

The FCA's Proposed Guidance requires firms to "ensure there are no restrictions on the number of requests the firm, its auditor or the regulator can make access or receive data".[16]

We believe that it is important for relevant parties other than the firms themselves, e.g., their auditors or regulators, to have access to the data where appropriate. However, we also believe that the requirements as proposed could impose excessive costs on third parties and create data security and intellectual property risk. Allowing for an unlimited number of requests for unrestricted/effective access to data could result in a dramatic increase in storage, access and control costs. We therefore recommend that any such requests should be limited to cases where they are "reasonable".

Access to business premises

The FCA proposed that firms, auditors and regulators should have access to business premises including data centers of third parties.[17]

While it is natural for firms to visit the head offices of third parties as part of their due diligence process before they decide to make use of their services, we believe that regular visits to operations and data centers would create significant costs for third parties without a corresponding benefit. Moreover, some third parties outsource their hosting operations to public cloud providers that, by definition, use the same data centers to provide their services also to other, sometimes competing, firms. Firms' access to public cloud data centers could hence result in data protection issues for other firms that also use the cloud provider in question.

We therefore recommend that the FCA's Guidance only require visits by a reputable audit firm whose findings are provided upon request by the client of the third party. We believe that such approach would also ensure the operational costs of third parties managing these visits stay reasonable.

Relationship between service providers

The FCA proposed that, if the "regulated firm does not directly contract with the outsource provider, it should review sub-contracting arrangements to determine whether these enable the regulated firm to continue to comply with its regulatory requirements".[18]

Our experience has shown that sub-contracting arrangements made by third parties often contain sensitive information and third parties should therefore not generally be required to allow firms to review such arrangements. We recommend that third parties should instead be required to make representations of vendor risk assessments conducted by them on their sub-contractors. We believe that such approach should be sufficient for the due-diligence purposes of firms.

[15] Pg. 10
[16] Pg. 11
[17] Pg. 11
[18] Pg. 12

Resolution

The Proposed Guidance states that "Any services should be organised in such a way that they do not create additional complexity in a resolution and do not become a barrier to the resolution or orderly wind-down of a firm".[19]

We believe that, to be practical, this requirement should be limited to only the *critical* outsourcing services in the absence of which firms' orderly resolution would not be possible. Third parties should be allowed to terminate services which are not critical to the orderly resolution of the firm in question. Moreover, these arrangements should be contractually determined on the basis of mutual agreement between the third party and the firm about the criticality of the service.

Exit plan

Markit understands the importance of transitional provisions to ensure the continuity of firms' businesses which are dependent on services provided by third parties. However, these arrangements should apply only to critical outsourcing services that are essential to compliance with the regulatory regime"[20] to adequately protect the interest of third parties.

The proposals also require firms to have a "specific obligation put on the outsourcing provider to cooperate fully with both the firm and any new outsource provider(s) to ensure there is a smooth transition".[21] We believe that third parties should be expected to reasonably cooperate with the new outsource provider which should not amount to it revealing sensitive business practices to the new provider which might be a competitor of the third party in question. Moreover, third parties should be adequately compensated by firms for the transition services provided by it.

Finally, the proposals require a firm to "know how it would remove data from the service provider's systems on exit".[22] We believe this provision should be clarified to state that the removal of data should not mean that third parties be required to purge their systems of data on the outgoing firm. Such clarification would be particularly important for third parties that operate on a shared service[23] model where any removal of data of the outgoing firm could result in negative consequences for other firms on the platform.

****

We hope that our above comments are helpful to the FCA. We would be more than happy to elaborate or further discuss any of the points addressed above in more detail. In the event you may have any questions, please do not hesitate to contact us.

Yours sincerely,

[19] Pg. 13
[20] Pg. 14
[21] Pg. 14
[22] Pg. 14
[23] Shared services centralises operational functions, originally performed in separate divisions or locations of a company, with economies of scale and standardisation of processes ultimately translating into cost savings. The strategy can also involve sharing services between two or more firms. 'Shared service' can span across different functional areas of the value chain including Finance, Operations, IT, Risk or Human Resources. Functions such as Reconciliations, Settlements or Clearing can be centralised under 'Shared Service'.

Marcus Schüler
Head of Regulatory Affairs
Markit
marcus.schueler@markit.com