Peter Adrian Kavounas
Cloud Strategix, LLC
202-288-2446 (o)

pkavounas@cloudstrategix.com
www.cloudstrategix.com

June 5, 2012

David Stawick
Secretary
Commodity Futures Trading Commission
1155 21st Street, NW
Washington, DC 20581

Re: **RIN 3038-AD83**; **Proposed Swap Data Repositories: Interpretative Statement Regarding the Confidentiality and Indemnification Provisions of Section 21(d) of the Commodity Exchange Act**

Dear Mr. Stawick,

This comment is being submitted on behalf of the data hosting and cloud computing industry. I appreciate the opportunity to submit the enclosed comments to the Proposed Swap Data Repositories ("SDR"): Interpretative Statement Regarding the Confidentiality and Indemnification Provisions of Section 21(d) of the Commodity Exchange Act ("CEA") by the Commodity Futures Trading Commission ("CFTC") in the Federal Register. 77 Fed. Reg. 88 (May 7, 2012).

While I support the CFTC's efforts to clarify provisions of section 21(d) so as to "not operate to inhibit or prevent foreign regulatory authorities from accessing data in which they have an independent and sufficient regulatory interest,"[1] the hosting industry is concerned that several costs, unintended consequences, and impracticalities may not have been fully considered by the CFTC in its interpretation. Additionally, as the costs and a possible solution – indeed, as the interpretation itself – are so heavily integrated to the final rule for Swap Data Repositories: Registration Standards, Duties and Core Principles, I have included an analysis of issues surrounding that regulation as well.

Essentially, this interpretative statement does not seem to consider the great cost to the data center that hosts the SDR in assisting the SDR with compliance with foreign regulators. More specifically stated, who bears the additional cost of storing data per a request by a foreign regulator, and who bears the cost of reporting that data to foreign

[1] CFTC Proposed Swap Data Repositories: Interpretative Statement Regarding the Confidentiality and Indemnification Provisions of Section 21(d) of the Commodity Exchange Act, Summary section, which allows the SDR to share potentially confidential information with foreign regulators without first obtaining an indemnification agreement.

regulators? If the SDR has a general or blanket indemnification with the data center that hosts it, but no specific indemnification for breach of confidentiality while operating in compliance with a foreign regulator, then the SDR can furnish confidential information about a data center without the data center even knowing that the SDR is an SDR. Additionally, there is an easy fix to this solution, which would be to exempt all independent data centers from this rule. However, that does not solve the problem of data center operational information being publicly disseminated by a foreign or domestic regulator: an entirely bigger problem presented by the final rule.

In order to understand this issue and solution, it is first important to explore some of the issues surrounding the underlying regulation.

I wish to share with you my thoughts regarding:

- Where SDRs are actually located (within data centers), and the relationship between SDRs and third-party provider data centers,
- The biggest unintended consequence of this interpretative statement,
- The inevitable effects, costs, and consequences to those third-party providers and the resultant damage to relationships to SDRs, and
- Some possible alternatives to the rule and to this interpretative statement so as to mitigate these consequences.

Background on Data Center Hosting; Relationship to SDRs

Independent data center companies[2] operate as technology infrastructure companies that provide data center facilities and managed services. Managed services provide management of security, network, systems, and applications, and offer colocation and database management. Its data center services include storage/tape backup, security, disaster recovery, load balancing, connectivity, and, of course, power.

This industry employs thousands of people nationwide, and is by all measures where the Internet is physically located.

For the portion of the business in the data hosting services category, the data center model is net-neutral, or content neutral. Net-neutrality allows data centers to host companies and new technologies without access or connection to customer traffic and content, let alone an ability to monitor such traffic. Ostensibly, these data centers let technology companies run their own services and merely provide access to the data center, but have no access to the ***data on these systems***.

[2] Independent data center companies are companies that host technology for cloud computing, financial services, health care, and other industries, as opposed to certain exchanges that are also data centers, such as the Chicago Mercantile Exchange.

Peter Adrian Kavounas
Cloud Strategix, LLC
202-288-2446 (o)
pkavounas@cloudstrategix.com
www.cloudstrategix.com

All contracts between data centers and their customers have confidentiality agreements between both parties, assuring the customer that its technology information will not be disclosed and that the data center's operational and business model will also will be kept confidential.

As they begin to register and operate, SDRs will undoubtedly be located within data centers. Some SDRs will be located in data centers hosted by swaps execution facilities ("SEF"), derivatives clearing organizations ("DCO"), or designated contract markets ("DCM").

However, some SDRs will be located, either entirely or in part, within independent data centers. The reasons could be anything from redundancy purposes (to have another location in case the data center where the exchange is located is "down" for some reason), or for cost, reliability, or connectivity reasons. Really, SDRs could locate in independent data centers for any number of purely economical, operational, or logistical reasons. But assuredly, all SDRs will be located in data centers potentially all over the nation and throughout Europe and Asia.

Additionally, as SDRs complete the registration process over the next several months, it is likely that many data centers are already hosting "soon to be" SDRs ***without even knowing their customers are SDRs***. Again, because data centers typically offer a product that requires that the data center not know what the customer is doing (net-neutrality), it is entirely possible that some of the companies applying to become SDRs will be granted registration, but will not inform the data center about this registration.

Nothing in the proposed interpretative statement, the final rule on Swap Data Repositories: Registration Standards, Duties and Core Principles,[3] or the Form SDR ***mandates that SDRs are required to inform the data center about their obligations or their status as SDRs***. In fact, many contracts between data centers and their customers have boilerplate legal language indemnifying each party for litigation due to regulatory compliance. Essentially, a data center could contract with an SDR, not know it, and only find out about this relationship when they find confidential operational information on a foreign regulator's website.

Main Unintended Consequence of this Proposed Interpretation and the Rule

As SDRs begin to report and fulfill their duties as SDRs, ***the confidentiality of the data centers hosting those SDRs will be breached, which could destroy the hosting industry's business model and prevent SDRs from operating***.

[3] 76 Fed Reg. 170, September 1, 2011; *see* Final Rule § 49.18 "Confidentiality and Indemnification Agreement" is strictly between SDR and its customers, or to those the SDR provides services.

Peter Adrian Kavounas
Cloud Strategix, LLC
202-288-2446 (o)
pkavounas@cloudstrategix.com
www.cloudstrategix.com

Both through the registration process and ongoing "maintenance" by foreign and domestic regulators, SDRs are required to supply information that is made public by the CFTC, domestic, and foreign regulators. The publishing of confidential information through an SDR's registration, which is entirely dependent on the proprietary operational standards of the data center that hosts the SDR, is a breach of the data center's confidentiality and, therefore, ***its hosting contract with the SDR***. Additionally, supplying a foreign regulator with potentially confidential information regarding data center operations and systems that are integrated into those of the SDR would be a breach of contract with the data center. Because it would not be required to sign an indemnification agreement before the SDR can turn over data to a foreign regulator, a data center would have no idea that such a breach occurred, let alone the fact that one of its customers was an SDR with these types of reporting requirements.

Final Rule "Swap Data Repositories: Registration Standards, Duties and Core Principle's 'Registration Instructions'", part 5 states that "information supplied on this form (Form SDR) will be included routinely in the public files of the Commission and will be available for inspection by any interested person."[4] First of all, this means that any information from the registration statement may be made public and may be made available to anyone, including ***a competitor to the data center, either domestic or foreign***.

As data hosting standards and practices, as well as intellectual property rights are vastly different oversees, this interpretative statement could open the door for foreign competitors to see what domestic data hosting companies are doing, and compete with potentially lower labor costs (such as those in India and China). Not only would the data centers lose, but also SDRs and the market in general might lose out to foreign competitors, who might end up providing very sensitive transactional market data with very little privacy and security protection, all in the name of lower costs to the end user.[5] Of course, that end user might not care about the monetary cost when all of its confidential trade information is breached due to lax security measures.

As the information on Form SDR may be made public, sections 30, 36, 37, 38, and 39 of "Exhibits III – Operational Capability" require SDRs to furnish confidential information about data centers.[6] Every piece of information in these sections – disaster recovery procedures, backup protocols, security, and network capability – is all in the purview of the data center, ***not the SDR that is leasing space and services from the data center***.

---

[4] 76 Fed Reg. 170, Appendix A to Part 49 – Form SDR, General Instructions (5). September 1, 2011.
[5] Privacy and security regulations in China are much looser than domestic regulations, which could be cause for concern to the CFTC in achieving its goal of market integrity.
[6] Id.; Form SDR, Exhibits III – Operational Capability.

Peter Adrian Kavounas
Cloud Strategix, LLC
202-288-2446 (o)
pkavounas@cloudstrategix.com
www.cloudstrategix.com

Therefore, by the very definition of registering and operating as an SDR, a company must furnish confidential operational information about the independent data center hosting that SDR, thereby, breaching its contract with the data center.

Inevitable Effects, Costs, and Consequences to Data Centers and Damage to Relationships with SDRs

The final rule requires that SDRs inform their customers, but, indeed, the data center is not a customer of the SDR. Rather, the SDR is a customer of the data center, the data center having no idea what the SDR is doing, which is accepting, normalizing, and storing trade execution data in the data center's facility.[7]

Since pure play, independent data centers will host SDRs, it is necessary to examine what this means for the industry. In light of the proposed interpretative statement regarding foreign regulator access to SDR data, and, of course, domestic regulator access, it is important to keep in mind that the cost to store and report that data will be shouldered by the data center.

From its simplest perspective, customers of the SDR, market participants required to report to SDRs (such as major swaps participants, swaps dealers, etc.), and SDRs themselves share one characteristic that data centers do not: ***unlike data centers, they all chose to participate in this market, to bear the cost of participation, and to anticipate the costs associated with compliance.***

In light of these potential consequences, hosting an SDR could be catastrophic. This proposed interpretative statement and the SDR rules require public disclosure, as well as foreign and domestic regulatory disclosure, of operational information about the data center. The SDR will be furnishing this confidential information without even informing the data center that hosts the SDR.

The final rule requires that SDRs demonstrate processes and systems in place for data recovery, backup, security, and network capability (telecommunications connectivity speed).[8] Each of these services is controlled by the data center, not necessarily the SDR, depending on the relationship – content neutral versus managed services.

To the extent that data centers control these aspects of the SDRs business, then the SDR would have to report on the data centers' abilities to perform in each area mentioned. Typically, both customers and data centers sign confidentiality agreements so that neither party can disseminate confidential operational and business model information such as that required on the Form SDR.

---

[7] 76 Fed Reg. 170, §§ 49.18, 49.26 referring to written agreements from customers and disclosure requirements of SDRs to customers, respectively.
[8] 76 Fed Reg. 170, Appendix A to Part 49 – Form SDR, Exhibits III – Operational Capability.

However, under this rule and proposed interpretative statement, SDR compliance mandates ***breaching confidentiality of the data center's operations by disclosing privileged company information to foreign and domestic regulators***. Most of this information, which consists of unique network designs and system integrations, is patented for the sole reason that no system is the same. Therefore, some data centers make money based on the setup of the data center and the value this adds to its customers for the purposes of backup, recovery, speed, and all the other reasons an SDR would be located in an independent data enter in the first place.

If this rule or the interpretative statement were enforced, then data centers will begin to avoid signing SDRs as customers for fear of having confidential operational information disclosed. Then, every SDR will have to either colocate with a SEF, DCM, or DCO at a typically much higher rate then that of an independent data center (typically it is 10x factor for leasing space from an exchange rather than an independent data center).

In the alternative (and it is not a good one), the SDR will be forced to build its own data center. Building a data center is an 18-month process, and requires a $50 million cash outlay at the low end.

Once SDRs begin to operate on their own (incurring the costs of storage, backup, recovery, etc.), these expensive alternatives will incentivize SDRs to stop operating as SDRs so as to not have to comply with these costly unintended consequences of the rule and interpretative statement. Coupled with the fact that some foreign regulators may publish or otherwise disseminate confidential operational data center information creating a large foreign SDR and data center market, these alternatives are very costly and extremely likely to occur.

Those are two very real results from this interpretative statement and the rule.

What has the CFTC decided should happen when the SDRs no longer want to be SDRs? Who will then be required to host, normalize, and store this data? Will the CFTC bear the enormous cost of storing all the data for every trade? Will the CFTC require the SEF, DCO, or DCM to bear this cost on its own if it wants to be a SEF, DCO, or DCM? And, if this requirement is attached to the SEF, DCO, or DCM registration, can the CFTC trust that the SEF, DCO, or DCM will accurately report data from it own trades with no independent oversight or checks in place?

Alternatives to Proposed Interpretative Statement

There should be a requirement that, to operate as an SDR, the owners and operators of the facility which hosts the SDR must be informed. This could easily be an amendment to rule §49.26, by stating (added language in bold italics):

Peter Adrian Kavounas
Cloud Strategix, LLC
202-288-2446 (o)

pkavounas@cloudstrategix.com
www.cloudstrategix.com

> Before accepting any swap data from a reporting entity or upon a reporting entity's request, a registered swap data repository shall furnish to the reporting entity ***and to the data hosting provider of the swap data repository*** a disclosure document that contains the following written information, which shall reasonably enable the reporting entity ***and the data hosting provider*** to identify and evaluate accurately the risks and costs associated with using the services of ***or with hosting and providing services to*** the swap data repository.[9]

Data centers have their own set of standards for security, network capability, backup, and disaster recovery. Do not proceed with a rule measuring the industry without considering what the industry standard is, much less how the industry experts measure such criteria.

To solve this problem, the CFTC and foreign regulators should not finalize any other interpretative statement or regulation regarding this market without contacting and engaging with industry experts; the independent data hosting companies.

The issue regarding the indemnification of SDRs by data centers that do not even know what they are indemnifying can be easily solved: provide an exemption for all data centers to indemnify SDRs for regulatory inquiries, enforcement proceedings, or litigation for both foreign and domestic regulators.

* * * * * *

As I represent independent data hosting companies, I would be happy to discuss these issues further. It is difficult to imagine the success of the swaps market without the fervent participation of the industry experts who will be hosting and transmitting all of the data surrounding this market.

For the reasons outlined above, the data hosting industry would like to offer its expertise in furtherance of the goals of the CFTC and, indeed, the Dodd-Frank Act.

If you have any questions, or wish for clarification on any of these matters, please do not hesitate to contact me.

Sincerely,

Peter Adrian Kavounas
CEO and President
Cloud Strategix, LLC

[9] 76 Fed Reg. 170, §49.26. September 1, 2011.