620 8th Avenue
35th Floor
New York, NY 10018
United States

+1 212 931 4900 Phone
+1 212 221 9860 Fax
ihsmarkit.com

Submitted electronically via www.regulations.gov

Robert deV. Frierson
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

Legislative and Regulatory Activities Division
Office of the Comptroller of the Currency
400 7th Street SW
Suite 3E-218, mail stop 9W-11
Washington, DC 20219

Robert E. Feldman
Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street NW., Washington, DC 20429

February 17, 2017

Enhanced Cyber Risk Management Standards

To Whom It May Concern,

IHS Markit appreciates the opportunity to comment on the Board of Governors of the Federal Reserve System ("Board"), the Office of the Comptroller of the Currency ("OCC"), and the Federal Deposit Insurance Corporation's ("FDIC") (collectively the "Agencies") joint advance notice of proposed rulemaking concerning "Enhanced Cyber Risk Management Standards" ("ANOPR").[1] We share the concern that "[a]s technology dependence in the financial sector continues to grow, so do opportunities for high-impact technology failures and cyber-attacks."[2]

IHS Markit[3] (Nasdaq: INFO), is a world leader in critical information, analytics and solutions for the major industries and markets that drive economies worldwide. The company delivers next generation information, analytics and solutions to customers in business, finance and government, improving their operational efficiency and providing deep insights that lead to well-informed, confident decisions. IHS Markit has more than 50,000 key business and government customers, including 80 percent of the Fortune Global 500 and the world's leading financial institutions. IHS Markit has been actively and constructively engaged in the debate about regulatory reform in financial markets, including topics such as the implementation of G20 commitments for OTC derivatives and the design of a regulatory regime for benchmarks. Over the past years, we have

[1] Enhanced Cyber Risk Management Standards, 81 Fed. Reg. 74,315 (Oct. 26, 2016), https://www.occ.gov/news-issuances/news-releases/2016/nr-ia-2016-131a.pdf.
[2] Id.
[3] For further information, please visit http://www.ihsmarkit.com/

submitted more than 150 comment letters to regulatory authorities around the world and have participated in numerous roundtables.

IHS Markit provides a variety of third-party "fintech" services to banks, other market participants, and market infrastructures, for example:

- *Post-trade services*: facilitating compliance with best execution requirements[4] and margin calculation requirements.[5] IHS Markit's post-trade processing service also facilitates compliance with Commodity Futures Trading Commission ("CFTC") and other regulatory regimes' derivatives reporting and confirmation requirements, among other regulatory requirements, in addition to facilitating clearing, providing operational efficiencies, and mechanisms for risk mitigation that come from utilizing IHS Markit's trade processing platform.[6] It should be noted and emphasized that IHS Markit is actively working with other industry stakeholders to leverage distributed ledger technology ("DLT") and blockchain technology more generally.[7]

- *Managed services*: facilitating due-diligence on their counterparties,[8] trading algorithms,[9] and vendors.[10] Other IHS Markit services assist firms in complying with tax regulations.[11]

- *Pricing, liquidity, reference, and valuation data*: IHS Markit provides pricing, liquidity reference, and valuation data that is used in different use cases, e.g., trading, post-trade, risk, and regulatory and accounting compliance contexts.

Among the post-trade services IHS Markit provides is a "third-party hub" service for processing derivatives.[12] IHS Markit's third-party hub service, also known as "MarkitSERV," provides bank, buyside, corporate, brokers, and execution platform customers a single point of connectivity to 16 derivatives clearinghouses worldwide, eliminating the need for firms to establishing and maintaining serial connections and application programming interfaces ("APIs") with each clearinghouse, creating a single workflow for all post-trade processing needs, including regulatory reporting and the processing of executed and cleared trades into back office systems. Globally

---

[4] As required, for example, under MiFID 2. See https://www.markit.com/Product/Transaction-Cost-Analysis

[5] This is required, for example, under the EMIR and Dodd-Frank risk mitigation techniques for uncleared derivatives. See https://www.markit.com/product/analytics

[6] See https://www.markitserv.com/assets/ms-en/docs/presentations/MarkitSERV_for_EMIR_Regulatory_Reporting_presentation.pdf.

[7] To provide a publicly discussed example, see Bitcoin's Blockchain Technology Proves Itself in Wall Street Test, Apr. 7, 2016, http://www.wsj.com/articles/bitcoins-blockchain-technology-proves-itself-in-wall-street-test-1460021421.

[8] Provided by IHS Markit's KYC.com platform.

[9] The IHS Markit Counterparty Manager platform ("MCPM") helps firms perform due diligence on trading algorithms used by their executing brokers. This is a requirement, for example, in Hong Kong and under MiFID 2.

[10] Firms perform due diligence on their third party vendors as part of their business continuity and disaster planning programs. See http://www.ihsmarkit.com/product/ky3p for more details.

[11] Our platforms help firms comply with "Common Reporting Standards" (see http://www.markit.com/Product/File?CMSID=675f66d146e94986ad043d78f47e3558) as well as with the Foreign Account Tax Compliance Act (FATCA) requirements. See https://www.markit.com/Product/Fatca-Service-Bureau

[12] "Currently, [swap] trades can be promptly submitted directly to DCOs either through a direct connection between the SEF or DCM and the DCO or the use of a third-party service provider acting as agent for the SEF or DCM." CFTC No-Action Letter 15-67, Dec. 21, 2015, http://www.cftc.gov/idc/groups/public/@lrlettergeneral/documents/letter/15-67.pdf.

over 2,000 firms use IHS Markit's trade processing platforms that process, on average, 90,000 derivatives transaction processing events every day.

I. General Comments

While we welcome the ANOPR and the agencies' focus on cyber risk management as timely and necessary, we seek clarification regarding certain aspects of the ANOPR, particularly as it relates to third-party service providers like IHS Markit. The ANOPR considers "whether to apply the standards to third-party service providers with respect to services provided to depository institutions and their affiliates that are covered entities (covered services)."[13] The rationale for this concept is to "ensure consistent, direct application of the standards regardless of whether a depository institution or its affiliate conducted the operation itself, or whether it engaged a third-party service provider to conduct the operation."[14]

We would recommend that in any proposal based on the ANOPR that the Agencies more clearly describe their expectations as it relates to covered service providers ("CSPs"). For example, we would ask that any such proposal address the following questions:

- What services would be considered "covered services?" In theory, any dependence on a third-party service involving cyber technology could create cyber risk, e.g., any type of software program, hardware technology, etc. We think more thought should be given to where to draw the line between covered services and non-covered services.

- For CSPs, would the cyber risk management standards apply on a service or enterprise level? As discussed in our answer to Question 2 below, we think the standards should apply at the service level provided certain precautions to contain cyber risk are taken.

- Would the five (5) enhanced cyber risk management standards apply to CSPs? If so, to what extent? For example, would the cyber risk governance requirements, e.g., a requirement that the board of directors approve the cyber risk management program, apply to CSPs? We would recommend that the Agencies in any proposal carefully describe the expectations as it relates to CSPs more explicitly in any proposal.

Finally, with respect to CSPs that may be "sector-critical systems," we would recommend clarifications of what activities "support the clearing and settlement" of derivatives transactions and that the two-hour RTO requirement be phased in over the course of three years if it is deemed necessary for sector-critical systems that "support the clearing and settlement" of derivatives.

II. Discussion

Below we provide our comments in response to specific questions posed by the ANOPR.

QUESTIONS ON THE SCOPE OF APPLICATION

2. What are the costs and benefits of applying the standards to covered entities on an enterprise-wide basis? If the agencies were to consider exempting certain subsidiaries within a covered entity from the standards, what criteria should be used to assess any such exemptions? What safeguards should the agencies

[13] Id. at 74,318.
[14] Id.

require from a subsidiary seeking to be exempted from the standards to ensure that an exempted subsidiary does not expose the covered entity to material cyber risk?

We would seek clarification that the enhanced cyber risk standards apply only to covered entities on an "enterprise-wide" basis while for CSPs, the standards apply at a covered service level so long as reasonable precautions, focusing on the security perimeter of such covered services are taken to protect the covered service from cyber risks from elsewhere in the service providers' enterprise.

4. What are the most effective ways to ensure that services provided by third-party service providers to covered entities are performed in such a manner as to minimize cyber risk? What are the advantages and disadvantages of applying the standards to services by requiring covered entities to maintain appropriate service agreements or otherwise receive services only from third-party service providers that meet the standards with regard to the services provided, rather than applying the requirements directly to third-party service providers?

The most effective way to ensure covered services ae performed in a manner designed to minimize cyber risk is to focus on the security perimeter and points of entry into the covered service. We think that this could be done cost effectively through a requirement for covered entities to negotiate a standard covered services agreement designed to comply with the standards eventually adopted by the Agencies.

With respect to "applying the requirements directly to third-party service providers," we seek clarification how the Agencies have statutory authority to do this and are not convinced that approach is warranted. If such statutory authority is sought, we would recommend coordinating the approach with other regulators with existing third-party service provider-related rules or standards. If the Agencies intend to apply the standards "directly" without statutory authority, they should make CSP compliance voluntary and optional, i.e. sufficient but not necessary, for banks utilizing CSP services.

Moreover, if standards are applied directly to CSPs, the prescribed cybersecurity protections would likely either be too low or too high. The best approach would be principles-based and defer to the bank to determine the applicable cyber risks and how best to manage such risks. For example, with respect to data privacy, individually negotiated agreements with covered entities are best to ensure personal data is protected. If cyber risk management standards are applied directly on CSPs, then they should reflect a minimum standard with banks to determine whether heightened standards should apply.

5. What are the advantages and disadvantages of applying the standards directly to service providers to covered entities? What challenges would such an approach pose?

The primary advantage, from our perspective, of directly applying the standards to service providers would be the reduction of time needed to negotiate service agreements on an ad hoc, bilateral basis with covered entities. We think an indirect approach to applying standards, via the covered entities, can and should be streamlined through a standard agreement and dialogue

between covered service providers and the Agencies. We commend the OCC for recently publicly indicating its intention to commence precisely such a dialogue.[15]

The primary disadvantage of directly applying the standards to service providers is the risk of redundant, conflicting, or disproportionate regulation. This risk could be mitigated by a harmonized approach across the different financial regulators, including the Agencies and the CFTC and SEC, as well as any other financial regulator with respect to covered service providers.

6. What factors are most important in determining an appropriate balance between protecting the safety and soundness of the financial sector through the possible application of the standards and the implementation burden and costs associated with implementing the standards?

We think a principles-based approach with regular guidance and transparent decision-making as expectations are adjusted is the best way to ensure that the standard are proportionate and adapt promptly to changes in context. Whether standards are applied to CSPs directly or indirectly, we would caution that they be applied in a manner proportionate to the relevant cyber risk. For example, if a CSP is dealing with anonymous, de-identified, or otherwise non-personal data information, then risks are lower relative to a scenario where the CSP has financial account numbers, full names, etc.

We would recommend therefore that CSPs (and firms) should be given discretion to risk weight their cyber risk management program so that the most critical systems receive the most in terms of risk management oversight and resources while less critical systems are not rendered unduly expensive to operate.

21. How would the proposed standards for internal and external dependency management impact a covered entity's use of a third-party service provider?

We understand that many firms that would be affected by the ANOPR currently apply similar standards to manage vendor risk. We note that the costs to both affected firms and CSPs could be mitigated by facilitating dependency management.

There are third-party services available that can help affected firms and CSPs facilitate compliance with extant external dependency management requirements. Among the services IHS Markit provides its customers is its "Know Your Third Party" or "KY3P" platform.[16] KY3P is the first centralised, cloud-based data hub that simplifies and standardizes third party risk management processes focusing on vendor due diligence and ongoing monitoring. KY3P helps firms collect and maintain information, including corporate profiles and questionnaire responses from third parties. KY3P also actively monitors and reports of industry wide events, such as cyber risk-related events to its customers.

30. What impact would a two-hour RTO have on covered entities' use of third-party service providers? What challenges or burdens would be presented by the requirement of a two-hour RTO for covered entities who rely on third-party service providers for their critical systems? How should the agencies weigh such costs

[15] See OCC Recommendations and Decisions for Implementing a Responsible Innovation Framework, Oct. 2016, https://www.occ.gov/topics/bank-operations/innovation/recommendations-decisions-for-implementing-a-responsible-innovation-framework.pdf.

[16] See IHS Markit KY3P, http://www.markit.com/product/ky3p.

against other costs associated with implementing the enhanced standards outlined in this ANPR?

With respect to the impact of the two-hour RTO on third-party service providers, we comment below, first, regarding the scope of the sector-critical system requirements, including the two-hour RTO, and second, regarding the burden that such a requirement would have. We understand that many bank customers utilize IHS Markit's third-party hub services for more than five (5%) percent of their exchange-traded and OTC derivatives clearing and settlement and would therefore come under the requirements applicable to CSP sector-critical systems.

Regarding the scope of the sector-critical system standards, we note the ANOPR considers classifying as "sector-critical systems" third-party systems that "support the clearing or settlement of at least five percent of the value of transactions (on a consistent basis) in other markets (for example, exchange-traded and over-the-counter derivatives). With respect to CSP "sector-critical systems" for derivatives markets, we provide the following two suggestions:

1. We would recommend the Agencies to clarify that that the sector-critical threshold be based on the value of transactions (total notional amount executed) in exchange-traded and over-the-counter ("OTC") derivatives separately in order to ensure that all third-party systems relied upon by covered entities be subject to the heightened standards expected of sector-critical systems. This would ensure that the derivatives markets would have few weak cybersecurity links.

2. We would recommend the Agencies clarify their meaning when they describe "support[ing] clearing and settlement" noting that the CFTC and Securities and Exchange Commission ("SEC") and other regulators define these terms differently.[17]

3. We would recommend the Agencies clarify that "derivatives" be defined to include all products subject to the jurisdiction of the CFTC and security-based swaps subject to the jurisdiction of the SEC. The Agencies should also clarify that these standards would apply to distributed ledger and other new technologies utilized by banks in order to ensure the soundness of new infrastructures at the earliest stages of development.

4. We would recommend the Agencies carefully determine whether a two-hour RTO is necessary for sector-critical systems that support the clearing and settlement of derivatives. We note that currently we have developed a four-hour RTO standard for our processing business generally. This four-hour RTO is currently deemed by our customers

[17] See e.g., Clearing Agencies, https://www.sec.gov/divisions/marketreg/mrclearing.shtml ("Clearing Agencies are self-regulatory organizations that are required to register with the Commission. There are two types of clearing agencies – clearing corporations and depositories. Clearing corporations compare member transactions (or report to members the results of exchange comparison operations), clear those trades and prepare instructions for automated settlement of those trades, and often act as intermediaries in making those settlements. Depositories hold securities certificates in bulk form for their participants and maintain ownership records of the securities on their own books."). See also Interpretation: Confirmation and Affirmation of Securities Trades; Matching (1998), Rel. No. 34-39829; File No. S7-10-98, https://www.sec.gov/rules/interp/34-39829.htm ("The Commission is of the view that matching constitutes a clearing agency function within the meaning of the clearing agency definition under Section 3(a)(23) of the Exchange Act. 6 Specifically, matching constitutes "comparison of data respecting the terms of settlement of securities transactions." The Commission concludes that matching is so closely tied to the clearance and settlement process that it is different not only in degree but also different in kind from the current confirmation and affirmation process.")

as sufficient to support the processing, clearing, and settlement of transactions processed on our platforms. We would be happy to describe how our standards reflect customer demand and market discipline in further detail if this would be helpful.

31. How should the agencies implement the two-hour RTO objective? For example, would an extended implementation timeline help to mitigate costs, and if so, what timeline would be reasonable?

For CSP sector-critical systems, we would recommend that the two-hour RTO requirement be phased in over the course of at least three years. This would ensure a cost-effective transition and thorough implementation of new RTO requirements.

32. Should different RTOs be set for different types of operations and, if so, how? Should RTOs be expected to become more stringent over time as technology advances?

The two-hour RTO should only apply to the systems that actually "support the clearing and settlement" of derivatives transactions. The test for this is if the system failed, whether clearing and settlement would be substantially disrupted.

****

We hope that our comments are helpful to the Agencies. 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 Salman Banaei, Director and Head of Regulatory Affairs for North America, at salman.banaei@ihsmarkit.com or +1 347.324.8818.