February 20, 2014

Committee on Payment and Settlement Systems
Bank for International Settlements
4002 Basel
Switzerland
cpss@bis.org

General Secretariat
International Organization of Securities Commissions
C/ Oquendo 12
28006 Madrid
Spain
fmi@iosco.org

Re: Consultative Report—*Principles for Financial Market Infrastructures: Assessment Methodology for the Oversight Expectations Applicable to Critical Service Providers*

Dear Sirs:

The Clearing House Association L.L.C. ("Association") and The Clearing House Payments Company L.L.C. ("PaymentsCo," and, together with the Association, "The Clearing House")[1] are please to comment on the consultative report published jointly by the Committee on Payment and Settlement Systems ("CPSS") of the Bank for International Settlements and the Board of the International Organization of Securities Commissions ("IOSCO") entitled *Assessment Methodology for the Oversight Expectations Applicable to Critical Service Providers* ("Report").[2] The Report follows on the CPSS and IOSCO's *Principles for Financial Market Infrastructures* ("PFMI").[3] Annex F of the PMFI noted that "[a] regulator, supervisor, or overseer of an FMI *may* want to

[1] Established in 1853, The Clearing House is the nation's oldest banking association and payments company. It is owned by the world's largest commercial banks, which collectively employ 1.4 million people in the United States and hold more than half of all U.S. deposits. The Clearing House Association is a nonpartisan advocacy organization representing—through regulatory comment letters, amicus briefs, and white papers—the interests of its owner banks on a variety of systemically important banking issues. Its affiliate, The Clearing House Payments Company L.L.C., provides payment, clearing, and settlement services to its member banks and other financial institutions, clearing almost $2 trillion daily and representing nearly half of the automated-clearing-house, funds-transfer, and check-image payments made in the United States. See The Clearing House's web page at www.theclearinghouse.org for additional information.

[2] Available at http://www.bis.org/publ/cpss115.pdf.

[3] Available at http://www.bis.org/publ/cpss101a.pdf.

establish expectations for an FMI's critical service providers in order to support the FMI's overall safety and efficiency"[4] and set standards for the service providers in five areas. The assessment methodology is designed as a way to ensure that critical service providers meet the standards of Annex F—if an authority chooses establish those standards.

The Report notes that if an authority does adopt the standards for critical service providers,

> adherence to these expectations can be achieved in one of two ways, at the discretion of the authority: (a) the authority monitors adherence to the expectations itself in a direct relationship with the critical service provider or (b) the authority communicates the standards to the FMI, which obtains assurances from its critical service providers that they comply with the expectations.[5]

In either case, assessment would be done by the service provider itself or someone under its direction, with the completed assessment then provided to the FMI or regulator.[6]

SUMMARY

We urge CPSS and IOSCO not to adopt the proposed assessment methodology for the following reasons:

1. Regulators will likely have no authority to require critical service providers to undergo the self-assessment.

2. FMIs do not have the market power to enforce these standards on their critical service providers.

3. The proposed assessment methodology is too rigid and inflexible.

4. FMIs already monitor key performance metrics of critical service providers.

DISCUSSION

[4] PFMI at 170 (emphasis added).

[5] Report at 1.

[6] *Id*. at 2.

1. Regulators will likely have no authority to require critical service providers to undergo the self-assessment.

In the United States, regulation of financial market utilities ("FMUs") is governed by Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act.[7] Under that act, the Financial Stability Oversight Council designates FMUs as systemically important. FMUs that have been designated are then subject to enhanced regulation by a federal supervisory agency, which can be the Securities and Exchange Commission, the Commodity Futures Trading Commission, or the Board of Governors of the Federal Reserve System or another financial-institution supervisor.[8] These agencies have limited powers as specified by statute, and none of them are given any regulatory authority over telecommunications carriers, technology service providers, or similar concerns and therefore have no legal authority to impose on the service providers the standards set out in Annex F; nor can they insist that the service providers perform self-assessments against the standards in order to assure the supervisors of their adherence to the standards.

Given this lack of regulatory authority (which we believe may be true in a number of other countries as well), supervisors will be in no real position to "monitor[s] adherence to the expectations . . . in a direct relationship with the critical service provider."

This does not mean that governments are indifferent to—or lack the ability to—require technology and telecommunications companies, and similar critical infrastructures, to meet minimum standards of security and resilience. In the United States, public policy is to strengthen the security and resilience of its critical infrastructure against physical and cyber threats. The Secretary of Homeland Security has been directed, to, among other things, "[c]onduct comprehensive assessments of the vulnerabilities of the Nation's critical infrastructure in coordination with" other government agencies and the private-sector owners of those infrastructures.[9] The President has also issued an executive order calling for "a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards,"[10] and within the past week, the National Institute on Standards and Technology issued a framework for addressing the security of critical infrastructures that "focuses on using business drivers

---

[7] 12 U.S.C. §§ 5461–5472.

[8] *Id*. § 5461(8).

[9] Presidential Policy Directive / PPD-21 at 3 (Feb. 12, 2013), available at http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[10] Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes."[11]

2. FMIs do not have the market power to enforce these standards on their critical service providers.

If supervisory authorities are not in any position to enforce standards on service providers, the FMIs are even less so. Not only do they lack regulatory authority, they lack sufficient market power to induce the service providers to provide assurances of their adherence to the standards. Many of the corporations that provide critical telecommunications and technology services are large enterprises with billions of dollars in profits and millions of customers, many of whom are themselves major institutions. In addition, most critical service providers do not have a lot of competition for the services they provide.

By contrast, most FMIs are relatively small operations with few employees, small profits, and generate insignificant revenues for the service providers. They have virtually no market power to require the service providers to comply with the standards.

Because of these factors, it would be inappropriate for regulators (who have no authority over service providers) to require FMIs to obtain assurances of compliance from their critical service providers.

3. The proposed assessment methodology is too rigid.

The assessment methodology is a set of questions in the manner of an examination manual that seeks to elicit information about the procedures that a provider has to ensure its compliance with the relevant principles. While the Report states that "[t]hese questions are neither intended to serve purely as a checklist nor to be exhaustive," it contemplates additional questions, not fewer or different ones.[12] The service provider is expected to rate itself using the framework developed in the CPSS-IOSCO report, *Principles for Financial Market Infrastructures: Disclosure Framework and Assessment Methodology* (i.e., rate itself as observing, broadly observing, partly observing, or not observing each of the principles)[13]. Service providers are also

---

[11] National Institute of Standards & Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, at 1 (Feb. 12, 2014), available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[12] *See* Report at 2.

[13] CPSS & IOSCO, *Principles for Financial Market Infrastructures: Disclosure Framework and Assessment Methodology* at 10 (available at http://www.bis.org/publ/cpss106.pdf).

encouraged to publish their responses to the assessment methodology's questions, but this is not required.[14]

The result is a rigid method that seeks to push all service providers into the same categories, covering the same issues regardless of the service provided. Moreover some of the questions address issues that the service providers are likely to consider highly confidential. For example, Q 2.6 seeks information on policies and procedures for (a) granting logical and physical access to systems, (d) avoiding security breaches, and (e) protecting systems against attack. Release of this information could increase risk by making a service provider's systems more susceptible to successful attack—attacks that could implicate an FMI's essential services or data.

4. FMIs already monitor key performance metrics of critical service providers.

While, as noted, FMIs do not have significant market power with respect to their critical service providers, this does not mean that they do not do due diligence with respect to them. Critical service providers are monitored for financial strength and capability. FMIs will also monitor critical performance metrics. FMIs also seek—with varying degrees of success—information from the service providers about the resilience of their systems (e.g., multiple routing of telecommunications lines). FMIs will tailor these due diligence efforts to their specific needs—needs that are not necessarily captured by the proposed assessment methodology.

There is a real danger that if service providers are expected to conform to the assessment methodology, they will adopt them as a uniform response to all their FMI customers, becoming less responsive to the FMIs' individual needs. If this were to occur, it would increase rather than reduce FMI risk.

* * * * *

For the reasons stated above, we oppose the adoption of the proposed assessment methodology.

[14] *See* Report at 2.

If you have any questions about our comment, please contact me at joe.alexander@theclearinghouse.org or 212-612-9234.

Very truly yours,

Joseph R. Alexander
Senior Vice President, Deputy
General Counsel, and Secretary

cc: Ms. Louise L. Roseman
Board of Governors of the Federal Reserve System