Kathleen Cronin
Senior Managing Director, General Counsel
Legal Department

February 22, 2016

Submitted Via Agency Website http://comments.cftc.gov

Christopher Kirkpatrick
Secretary of the Commission
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street, NW
Washington, DC 20581

Re: Comment on RIN No. 3038-AE30, System Safeguards Testing Requirements

Dear Mr. Kirkpatrick:

CME Group Inc. ("CME Group"), on behalf of its four designated contract markets, its swap execution facility ("SEF") and its swap data repository ("SDR") welcomes the opportunity to comment on the Commission's proposed and advanced proposed rulemaking regarding System Safeguards Testing Requirements for DCMs, SDRs and SEFs (the "proposals").

CME Group is the parent of four U.S.-based derivative exchanges: Chicago Mercantile Exchange Inc. ("CME"), Board of Trade of the City of Chicago, Inc. ("CBOT"), New York Mercantile Exchange, Inc. ("NYMEX") and the Commodity Exchange, Inc. ("COMEX"). These Exchanges offer a wide range of products available across all major asset classes, including: futures and options based on interest rates, equity indexes, foreign exchange, energy, metals, and agricultural commodities. CME Group's exchanges serve the hedging, risk management and trading needs of our global customer base by facilitating transactions through the CME Globex® electronic trading platform, our open outcry trading facilities in New York and Chicago, as well as through privately negotiated transactions. CME Group operates a SEF, in addition to our current exchanges and trading platforms. Through its subsidiary CME, CME Group operates a provisionally registered SDR for the interest rate, credit, foreign exchange and other commodity asset classes and is responsible for the acceptance and maintenance of swap data as well as the dissemination of publicly reportable swaps. CME Group also includes CME Clearing, which provides clearing and settlement services for exchange-traded contracts as well as for over-the-counter derivatives transactions.

We appreciate the Commission providing the industry an opportunity to engage in an active discussion on the important topics around system safeguards and cyber security. Stability and reliability are core tenets of our business. Cyber security issues pose challenges that are greater than any one company and it is essential that the industry work together to

develop practical uniform goals with the ultimate policy objective of safeguarding the financial markets.

Program of Risk Analysis and Oversight

The Commission has proposed that, taking into account best practices and generally accepted standards, regulated entities maintain a systematized program of risk analysis and oversight with respect to its operations and automated systems. CME Group agrees with the Commission that a program of risk analysis and oversight based on an assessment of threats and vulnerabilities can identify and minimize sources of operational risk that could impact system integrity and better inform testing procedures, resulting in more appropriate and effective management of risks. CME Group already actively identifies and minimizes sources of operational risks stemming from the six categories identified in the Proposals, namely: 1) information security; 2) business continuity-disaster recovery ("BCDR") planning and resources; 3) capacity and performance planning; 4) systems operations; 5) systems development and quality assurance; and 6) physical security.

Best Practices

CME Group agrees that best practices and generally accepted standards must be considered within an overall program of risk analysis and oversight. We appreciate the Commission providing insight on the best practices and generally accepted standards it considers to be relevant, and request confirmation that other best practices and generally accepted standards also may be used in addition to or in lieu of those referenced in the proposal.[1] As a panelist at the Commission's roundtable discussion stressed, it is important to allow entities, especially those operating within multiple jurisdictions, the flexibility to look to best practices and standards most appropriate for addressing their unique risks.[2]

Many best practices and generally accepted standards, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, were created with broad applicability in mind and were not just designed for the financial services industry. Given the speed and agility of technological innovation, it may be challenging for published best practices and standards to remain current in the face of ever evolving risks.[3] The proposal recognizes that standards and best practices evolve over time. As a result, individual aspects of standards might best be suited to addressing an entity's risks, whereas other aspects may not be applicable. It is our understanding that the proposal does not seek to require that entities adopt

[1] See International Standards Organization ("ISO") 27002 Information Technology – Security Techniques (2013), for an example of another generally accepted standard.

[2] See CFTC Staff Roundtable on Cybersecurity and Systems Safeguards Testing (Mar. 18, 2015) at 198; see also 79 FR 72252 at 72300 (Dec. 5, 2014) (Regulation SCI final rule discussing the value of providing flexible guidance regarding the selection of best practices, and agreeing that such guidance should not be prescriptive).

[3] See 80 FR 76934 (Dec. 11, 2015) (National Institute of Standards and Technology (NIST) cybersecurity framework request for information (RFI)).

standards or practices in a prescribed, wholesale fashion. CME Group respectfully requests that the Commission specifically confirm the intent of its proposed requirement is that entities take into account best practices as they design their own tailored programs of risk analysis and oversight and not require the adoption of any particular set of standards in a wholesale fashion.

Enterprise Risk Management ("ERM") and Enterprise Technology Risk Assessments ("ETRA")

The Commission's proposal defines a seventh area, enterprise risk management and governance (ERM) programs designed to enable Board oversight of risks, including system safeguards related risks. The Commission proposes to require that entities address five areas with their ERM programs: 1) assessment, mitigation and monitoring of security and technology risk; 2) capital planning and investment with respect to security and technology; 3) board of directors and management oversight of system safeguards; 4) information technology audit and controls assessments; and 5) remediation of deficiencies.

CME Group requests the Commission confirm that it will continue to allow for flexibility in organizational design, allowing companies to determine the structure that most effectively addresses the operational components of these five coverage areas. CME Group believes that the Commission should not mandate a "one size fits all" approach, nor should it mandate that each component will be conducted by the ERM function. For example, the most effective way for some organizations to have ongoing and continual awareness of IT related risks may be for risk professionals to be embedded into the technology department; for others, it may be a centralized ERM function. Organizations should have the flexibility to place these functions into either the first or second line of defense depending upon their size, complexity, risk exposure, culture and other organizational specific factors, thereby promoting a culture that actively reviews risks and the mitigating controls that have been established. Similarly, an ERM program should facilitate reporting on risks related to capital planning for information security, but ERM would not be the function conducting the budgeting process itself.

We appreciate the Commission's flexible approach regarding both who must conduct an organization's ETRA and its particular methods, structures or frameworks. The proposal would require a written ETRA for covered DCMs and SDRs at least annually that takes into consideration different inputs including the results of testing of controls, and vulnerability testing. We agree that testing will greatly inform the ETRA process. We also agree that regular risk assessments should drive ongoing "risk management-based" efforts to address cyber risks.[4] ETRA written assessments, however, would benefit from a full cycle of controls testing, for which the Commission proposes at least a two-year cycle for covered DCMs and SDRs. CME estimates that, as proposed the ETRA would result in an approximate additional $500,000 per every two years.[5] CME Group respectfully requests that the requirement to complete a written

[4] See 80 FR 80140 at 80142 (Dec. 23, 2015) *citing* FINRA, Report on Cybersecurity Practices (Feb. 2015).

[5] This estimate does not separate out costs for clearing, trading or data reporting, but rather is a general estimate that encompasses potential additional costs for CME Group system safeguards controls testing as a result of the Commission's proposals.

assessment be aligned with an entity's frequency of controls testing. Allowing the ETRA to be conducted on the same schedule as controls testing would result in a more fully informed ETRA and would be more cost effective.

Finally, CME Group recognizes the importance of effective Board oversight and requests the Commission, in line with current industry practice, confirm that such oversight may be appropriately delegated to Board-level committees, such as Risk or Audit Committees, similar to other matters that have been assigned to committees such as internal controls and financial and compensation risk. We believe using a committee structure with reporting up to the full Board allows for more in depth reporting and analysis on the program and detailed discussions of key risks.

Cyber Security Testing Requirements for DCMs, SEFs and SDRs

The Commission's proposal identifies and proposes minimum standards for specific types of cyber security testing. CME Group agrees such testing is important to an entity's overall program of risk analysis and oversight.

Scope

The Commission proposes that cyber security testing scope be broad enough to "identify *any* vulnerability," which undermines the value of a risk based approach. The proposal's preamble places great emphasis on the important function of risk assessments, and describes testing as being informed by an entity's program of risk analysis and oversight. We strongly agree that organizations should use risk-based testing to adequately address potential vulnerabilities because it is practically infeasible to conduct testing designed to identify any potential vulnerability.[6] In accordance with industry best-practice, the Commission should make explicit in rule text that a risk based approach should be used to prioritize the identification and remediation of vulnerabilities. We strongly urge the Commission to clarify that testing be risked-based to focus on the most likely scenarios and highest value information assets. Further, an overly broad scope may result in the unintentional consequence that firms may incur outsized costs that do not yield commensurate benefits and/or distract firms from focusing more directly on the most critical items as they attempt to address any potential vulnerability, regardless of its risk. [7]

Finally, adopting regulatory language requiring registrants to identify any vulnerability underlies an assumption that companies falling victim to the most sophisticated threats are singularly responsible for being attacked. The Commission recognizes in its proposal that cyber threats increasingly emanate from sophisticated actors including criminal gangs and nation states, and that the velocity and number of attacks are growing exponentially. No one

[6] For example, on average there are 3-50 "bugs" per 1000 lines of code, any of which might result in a security concern. Windows operating system alone has approximately 50 million lines of code.

[7] See supra note 5 at 80141 (questioned the effectiveness of firewalls and discusses corporate information technology systems); but see 79 FR 72252 (permitting entities to segregate their environments to limit the scope of the regulation on a risk basis.)

company, regardless of its deep commitment or the strength of its controls, can single handedly address any potential vulnerability.[8] CME Group appreciates Commissioner J. Christopher Giancarlo's statements that Commission's proposals recognize that even the best defenses provide no guarantee of protection. We agree that adopting safe harbors for market participants who seek to comply with their core principle responsibilities will encourage market participants to seek out partnerships and will best serve the common goal of improving the industry's overall state of cyber resilience.

Independent Contractors

The Commission also seeks to require certain testing conducted by covered DCMs and SDRs be completed by independent contractors and for SEFs by independent professionals. The Commission's current 2012 final system safeguards rules provide flexibility regarding whether testing is completed by qualified, independent professionals who are either contractors or employees. Neither the Commission's 2012 rules, nor the proposed rule text clearly define either "independent contractors" or "independent professionals." The preamble discussion points without specific citation to best practices that call for testing by both employees and independent contractors. Best practices like NIST, however, recognize that independence is not determined by employment status, but rather by an individual's ability to conduct an impartial assessment. The FFIEC standards, the COBIT 5 framework and NIST all recognize that entity employees may conduct independent testing if they are not involved in the development, testing, or implementation of systems being reviewed.[9] CME Group agrees that certain types of testing should be conducted by persons who are not responsible for the development or operation of the systems or capabilities being tested, and thus are "independent" from those system operations.[10] CME estimates that if adopted as proposed, excepting controls testing costs that are discussed below, independent contractor requirements will result in approximately an additional $1.1 million every two years.[11] In lieu of requiring the use of external resources, testing may in certain cases be effectively conducted by independent employees within a company in a much more cost effective manner. Widely recognized models are discussed below for ensuring independence when conducting various types of testing.

---

[8] See Exec. Order No. 13636, 78 FR 11739 (Feb. 12, 2013); see also Exec. Order No. 13691, 80 FR 9347 (Feb. 20, 2015) (highlighting the need for a coordinated approach between the private sector and government regarding cyber threats).

[9] See The Federal Financial Institutions Examination Council ("FFIEC") IT Examinations Handbook, Operations (July 2004), available at *https://www.fdic.gov/regulations/information/information/ffiec.html*; ISACA Control Objectives for Information and Related Technology ("COBIT") 5 (April 2012), Monitor, Evaluate and Assess the System of Internal Control ("MEA") at MEA02.05; NIST Special Publication ("SP") 800-53 Rev.4, Security and Privacy Controls for Federal Information Systems and Organizations, (2013) ("NIST 800-53 Rev.4") (April 2013) at control CA-2.

[10] See 79 FR 72252 at 72343 (permitting reviews to be conducted by personnel not involved in the development, testing, or implementation of systems being reviewed).

[11] See supra note 4.

Vulnerability Testing

We agree with the Commission that vulnerability testing is critical to identifying and remediating potential vulnerabilities. Vulnerability testing should be embedded into an organization's systems development life cycle (SDLC), thereby promoting a culture of awareness as early and as close to the first line of defense as possible. The scope and frequency of vulnerability testing should be designed on a risk basis to provide focus on the most likely threats and most critical information assets. At least quarterly testing is likely an appropriate frequency for most organizations for their most critical assets.

The Commission's proposal, however, may result in some unintended consequences. Also, requiring the use of independent contractors may have unintended consequences that do not yield commensurate offsetting benefits. Allowing companies to use employees to conduct independent vulnerability testing has been proven to be effective, and also has the added benefit of promoting an internal culture that promotes and values the benefits of regular testing. While the strong benefits of promoting a culture of awareness is the primary reason for allowing employees to conduct independent vulnerability testing, there are other benefits to this approach as well. The Commission notes in its proposal that giving outsiders access to an organization's systems can introduce additional risk.[12] It has been suggested that proper vetting and contractual responsibility can help mitigate concerns, but once sensitive information has been disclosed in an unauthorized fashion, contractual remedies cannot undo the resulting security concerns. Further, there is a limited supply of qualified contractors that have the requisite skill sets to conduct vulnerability assessments and the costs associated with their retention may outweigh any realized benefits.

As a result, we respectfully request that the Commission continue to allow entities, taking into account their unique risk profiles, to use employees not involved in the development, testing or implementation of systems being reviewed to conduct vulnerability testing.

Penetration Testing

Penetration testing is a significant component of a DCM, SEF or SDR's program to identify and minimize sources of operational risk. We appreciate the proposal's flexibility regarding the design of penetration tests and believe that many risk based factors should inform the scope and frequency of this testing.

CME Group agrees that, taking into account risk, conducting external penetration tests on at least an annual basis generally will be appropriate. Familiarity with an entity's systems and capabilities makes testing completed by independent employees uniquely effective. Companies may find it challenging to recruit and retain employees capable of conducting internal penetration testing without introducing unnecessary risks into production and other sensitive environments because there is a scarcity of qualified professionals with that skill set.

[12] See supra note 5 at 80151 *citing* NIST Special Publication ("SP") 800-115, A Technical Guide to Information Security Testing and Assessment (2008) ("NIST 800-115") (Sept. 2008) at 6-6 (noting that giving outsiders access to an organization's systems can introduce additional risk, and recommending proper vetting and attention to contractual responsibility.)

As a result, the Commission should clarify that conducting annual internal penetration tests should be an objective, and not a strict requirement, so that organizations can prioritize effective testing done by independent employees over conducting testing at least annually simply to comply with a prescriptive testing frequency requirement.

Controls Testing

The Commission correctly identifies controls testing as a crucial part of a program of risk analysis and oversight, and we agree with the topical areas enumerated by the Commission: 1) information security; 2) business continuity and disaster recovery and planning and resources; 3) capacity and performance planning; 4) systems operations; 5) systems development and quality assurance; and 6) physical security and environmental controls.

As discussed above, we appreciate the Commission taking a flexible approach allowing organizations to use best practices and generally accepted standards to inform, but not dictate, the risk-based design and implementation of their controls testing. Controls testing should be tailored to each entity's systems and operations, taking into account an organization's risk assessments, and prioritizing those systems that directly support the regulated operations of an organization.[13] Controls testing will be more effective and cost efficient if organizations are able to focus and prioritize the underlying best practices used to design controls and the scope of testing applied to them.

Effective assessment of controls implementation may be conducted either by independent contractors or employees not involved in the development, testing or implementation of systems being reviewed. For example, under models for controls monitoring, testing and assurances for Sarbanes Oxley internal controls over financial reporting (SOX), it is well established that assessments may be conducted by professionals that maintain independence from the operation of the controls being tested but are also part of the same department or office. Assessment reporting is then conducted through an established governance structure that may include operating and business management, and ultimately oversight at the Audit Committee and/or Board level.

Requiring solely non-employee independent contractors to conduct testing, without involvement by employees, may not provide the most effective or efficient means for continued testing and enhancement of controls. For example, the proposal discusses organizations being in a state of "continuously" monitoring and evaluating the control environment.[14] CME Group believes that for some organizations this may best be achieved through a strong second line of defense that is embedded within, yet independent from, those responsible for the development or operation of the controls, systems or capabilities being tested. Strong familiarity with the development or operation of the controls, systems or capabilities being assessed is necessary to allow for efficient, continuous monitoring. Having compliance and other audit staff work alongside development and operational staff also helps promote a strong culture of compliance.

[13] See e.g. 79 FR 72252 at 72279 (permitting organizations to limit the scope of controls testing).

[14] See supra note 5 *citing* NIST SP 800-53A Rev.4, Assessing Security and Privacy Controls to Federal Information Systems and Organizations ("NIST SP 800-53A Rev.4") (Dec. 2014).

While the Commission proposes requiring independent contractor key controls testing for covered DCMs, strong familiarity with the systems or capabilities is even more important to ensure effective, continuous monitoring of the most critical or likely to quickly evolve areas. Involving external resources may be beneficial, but doing so should not exclude employees not involved in the development or operation of the controls, systems or capabilities being tested.

CME Group also agrees with the Commission that internal audit staff can provide a strong and independent third line of defense where the department is independent from management, objective in its findings, professional, and able to have free and unlimited access to the books, records and people of a company. It is common for the head of an organization's internal audit to be accountable directly to a Board-level committee and in fact to report to the Board-level Committee chairman. This reporting structure provides sufficient independence such that internal audit can fulfill its responsibilities as a third line of defense. These models have worked effectively in industry for other controls testing, such as SOX financial reporting control testing models.[15]

CME Group respectfully requests that the Commission permit organizations to design the frequency of their controls testing in line with their risk analysis, which may reasonably suggest that some less critical controls do not warrant testing on a two-year cycle.[16] Requiring testing of every control for every system on a short, prescriptive cycle may have the unintended consequence of having firms divert focus from higher risk or more evolving areas to lesser areas of risk to comply with the rule requirements. In short, controls testing should not be considered a "check-the-box" temporal exercise, but rather an ongoing and continuous enhancement activity that equally values assessment, testing and remediation. While we anticipate that many organizations will implement a key controls testing frequency schedule that is at least once every two years, maintaining flexibility regarding an organization's overall testing schedule will best serve the Commission's goals.

If the Commission does adopt a minimum frequency schedule for controls testing, we believe no more frequently than every three years would be a reasonable alternative. Unlike other proposed requirements, the Commission has recognized that complying with the proposed controls testing requirements for some DCMs and SDRs will result in additional costs. CME Group estimates that conducting controls testing in the manner proposed by the Commission will generally cost approximately an additional $5.6 million more over a two year period.[17] This estimate does not take into account the costs associated with any necessary remediation efforts. Adopting either a risk-based frequency of controls testing or a minimally less frequent requirement would make controls testing both more cost effective and would have the benefit of focusing on the most critical controls.

---

[15] See 79 FR 72252 at 72343 (recognizing this model by allowing independence to be defined not by employment status, but other factors like conflicts of interest to the system).

[16] See Office of Management and Budget, OMB Circular No. A-130, Management of Federal Information Resources (Nov. 28, 2000) (permitting federal agencies to test controls on a three year frequency); 79 FR 72252 at 72344 (assessments of systems are to be conducted once every three years).

[17] See supra note 4.

Finally, for some organizations engaging in controls testing in a meaningful and well organized way, full compliance with the scope and frequency requirements of the proposal will require not only a commitment of financial resources, but also adequate time to implement. The Commission has recognized that testing of too many controls in any one time period during the testing cycle would likely be unduly disruptive and burdensome without yielding a commensurate benefit. As a result, we respectfully request that the Commission adopt a reasonable implementation timeframe with respect to controls testing.

Security Incident Response Plan Testing

CME Group agrees with the Commission that maintaining a current, operable security incident response plan ("SIRP") is an important tool for all entities in their efforts to be ready to face inevitable cyber-attacks. CME Group maintains and regularly exercises its SIRP and believes that at least annual testing of the SIRP is appropriate. We appreciate the Commission taking a flexible approach regarding the format in which SIRP testing is conducted and agree that effective testing at different entities should take on the form that is best suited to address the unique risks faced by each organization.[18]

The Commission's proposal seeks to define security incidents broadly enough to capture both cyber and physical security events that actually or potentially jeopardize automated system operation, reliability, security or capacity, or the availability, confidentiality, or integrity of data. We agree with the Commission that testing should consider physical security incidents. We also appreciate the Commission recognizing the value of coordinating SIRP planning with other types of testing, for example crisis management plan testing, while at the same time permitting entities the flexibility to design their testing in the way that best addresses their unique risks.

The Commission's proposal seeks to require SIRP testing by either independent contractors or employees not responsible for development or operation of the systems or capabilities being tested. CME Group respectfully requests that the Commission permit an independent employee responsible for incident response may both design an organization's SIRP plan and be responsible for testing the plan. That employee would not be responsible for the development or operation of the functional systems or capabilities being tested. A company should be able to leverage its employees with expertise in crisis and risk management, and incident response and planning for both planning and testing purposes.

Business Continuity-Disaster Recovery Plans and Emergency Procedures

In a similar vein, we agree with the Commission's proposal that Business Continuity-Disaster Recovery (BCDR) plans and emergency procedures should be updated at least annually and more frequently if necessitated by other circumstances. CME Group places great value on maintaining effective and operable BCDR plans. Like the Commission, CME Group

[18] See e.g. NISTFramework for Improving Critical Infrastructure Cyber security v.1 (Feb.2014) (correctly emphasizing organizational structure, definition of roles and responsibilities, communication and escalation and not prescribing any particular response).

also values coordination of BCDR plans with the plans of market participants and essential service providers. CME Group is supportive of the FS-ISAC's recent efforts to develop a crisis handbook for the financial services industry to guide efforts in an industry-wide event.

Covered DCMs

The Commission should maintain a level playing field by adopting a uniform set of requirements for all DCMs. The proposed system to differentiate between covered DCMs and others is unnecessarily complex and imposes undue burdens. A reasonable alternative, in line with the proposal, would be for the Commission to adopt a flexible approach that allows testing frequency to be set in a risk-based manner. In practice, allowing risk-based testing frequencies should result in the same outcomes proposed in the rule, with the added benefits of retaining an approach capable of evolving over time and adopting a simpler, yet more effective, regulatory framework. Also, as discussed above, prescribing the use of independent contractors to conduct certain types of cyber security testing may result in unintended consequences. Finally, there is a high potential for undeserved yet negative reputational and other damage for the industry as a result of the public cyber-security failures of any DCM. In an extreme situation, a cyber-security related failure of any one DCM may fuel a perception that U.S. markets may not offer reliable, stable trade execution.

If the Commission adopts a covered DCM standard in its final rule, it should consider alternatives to the unnecessarily duplicative annual total trade volume reporting proposal. Under DCM Core Principle 8 and Part 16 of the Commission's regulations, the CFTC currently receives daily trade reports that provide information regarding volume. Requiring all DCMs to submit annual total trade volume reporting results in some DCMs taking on additional reporting obligations and related burdens (which provide absolutely no benefit to enhancing the systems safeguards capabilities) to support lesser regulatory burdens for competitors. A reasonable alternative that would not use resources that could be used to support operational safety and soundness is to allow DCMs the ability to "opt-in" to the covered DCM requirements in lieu of submitting the duplicative annual total trade volume reporting.

SEF ANPRM

Similar to DCMs, the Commission should adopt one risked based requirement for all SEFs. The Commission's proposal rightly places great emphasis on the importance of an entity's program of risk analysis and oversight and the ETRA process. Testing frequency should be determined based on a SEF's risk profile. The Commission should continue to require independent testing, but not prescribe the use of external contractors.

Systems Safeguards-Related Books and Records Obligations

We understand the supervisory need and respect the Commission's authority to require that records be provided. We respectfully request that the Commission continue its efforts to work with registrants regarding the manner in which highly sensitive materials are provided.

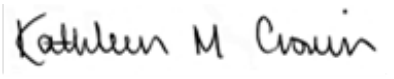
CME Group

Cost Estimates

Finally, the Commission's consideration of costs and benefits suggests that the proposed regulations will result in incremental costs and benefits. In February 2015, CME submitted information regarding systems safeguards testing costs requested by the Division of Market Oversight (DMO) and the Division of Clearing and Risk (DCR).[19] The cost estimates provided above regarding estimated additional costs that a registrant may incur as a result of the proposed requirements are in addition to the information previously submitted to DMO and DCR. CME estimates that the approximate additional costs over a two year period that may result from the proposals would total over $7.2 million, which we do not believe is an incremental amount. Again, this estimate does not separate out costs for clearing, trading or data reporting, but rather is a general estimate that encompasses potential additional costs for CME Group system safeguards controls testing as a result of the Commission's current proposals.

CME Group thanks the Commission for the opportunity to comment on the proposal and we look forward to a continued dialogue on the topic. Should you have any comments or questions regarding this submission, please contact Adrianne Joves by telephone at (312) 648-3891 or by e-mail at Adrianne.Joves@cmegroup.com.

Sincerely,



Kathleen M. Cronin

[19] This information was submitted along with a Freedom of Information Act (FOIA) Confidential Treatment request, pursuant to Commission Regulation 145.9(d)(ii).