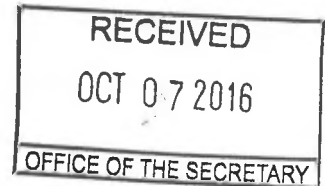


October 7, 2016

Brent J. Fields
Secretary
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090



Re: File Number 4-698
Notice of Filing of the National Market System Plan Governing the Consolidated Audit Trail

Dear Mr. Fields:

On April 27, 2016, the Securities and Exchange Commission (“SEC” or “Commission”) published the notice of the National Market System Plan Governing the Consolidated Audit Trail (“Plan”) for public comment. The SEC received 23 comment letters in response to the Plan. On September 6, 2016¹ and September 23, 2016,² the parties to the Plan – Bats BYX Exchange, Inc., Bats BZX Exchange, Inc., Bats EDGA Exchange, Inc., Bats EDGX Exchange, Inc., BOX Options Exchange LLC, C2 Options Exchange, Incorporated, Chicago Board Options Exchange, Incorporated, Chicago Stock Exchange, Inc., Financial Industry Regulatory Authority, Inc., International Securities Exchange, LLC, Investors’ Exchange LLC, ISE Gemini, LLC, ISE Mercury, LLC, Miami International Securities Exchange LLC, NASDAQ BX, Inc., NASDAQ PHLX LLC, The NASDAQ Stock Market LLC, National Stock Exchange, Inc., New York Stock Exchange LLC, NYSE MKT LLC, and NYSE Arca, Inc. (collectively, the “Participants”) – submitted responses to the issues raised in these letters. Pursuant to discussions with the SEC staff and the Participants’ ongoing analysis of the Plan, the Participants submit this letter to clarify certain aspects of the Plan, as set forth in detail in the Appendix. The Participants note that these clarifications represent the consensus of the Participants, but that all Participants may not fully agree with each response set forth in the Appendix.

¹ Letter from Participants to Brent J. Fields, SEC (Sept. 6, 2016) (the “September 6th Letter”).
² Letter from Participants to Brent J. Fields, SEC (Sept. 23, 2016) (the “September 23rd Letter”).

Brent J. Fields
October 7, 2016
Page 2

Respectfully submitted,

[Signature Pages Follow]

cc: The Hon. Mary Jo White, Chair
The Hon. Kara M. Stein, Commissioner
The Hon. Michael S. Piwowar, Commissioner
Mr. Stephen I. Luparello, Director, Division of Trading and Markets
Mr. Gary L. Goldsholle, Deputy Director, Division of Trading and Markets
Mr. David S. Shillman, Associate Director, Division of Trading and Markets

Bats BYX EXCHANGE, INC.

By: Tamara Schademann

Name: Tamara Schademann

Title: EVP, CRO

Bats BZX EXCHANGE, INC.

By: Tamara Schademann

Name: Tamara Schademann

Title: EVP, CRO

Bats EDGA EXCHANGE, INC.

By: Tamara Schademann

Name: Tamara Schademann

Title: EVP, CRO

Bats EDGX EXCHANGE, INC.

By: Tamara Schademann

Name: Tamara Schademann

Title: EVP, CRO

BOX Options Exchange LLC

By: *Bruce G. Goodhue*

Name: *Bruce G. Goodhue*

Title: *Chief Regulatory Officer*

Date: *10/4/2016*

ADDRESS FOR NOTICES:

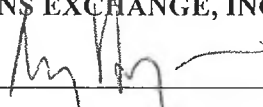
101 Arch Street, Suite 610

Boston, MA 02110

Facsimile: _____

Attention: _____

C2 OPTIONS EXCHANGE, INCORPORATED

By: 

Name: Greg Hoogasian

Title: Senior VP & Chief Regulatory Officer

CHICAGO BOARD OPTIONS EXCHANGE, INCORPORATED

By: 

Name: Greg Hoogasian

Title: Senior VP & Chief Regulatory Officer

CHICAGO STOCK EXCHANGE, INC.

By: 

Name: Peter D. Santori

Title: Executive Vice President
Chief Regulatory Officer


FINANCIAL INDUSTRY REGULATORY AUTHORITY, INC.

By: Marcia E. Asquith

Name: Marcia E. Asquith

Title: Senior Vice President and Corporate Secretary

INTERNATIONAL SECURITIES EXCHANGE, LLC

By: 

Name: John Zecca

Title: SR. Vice President

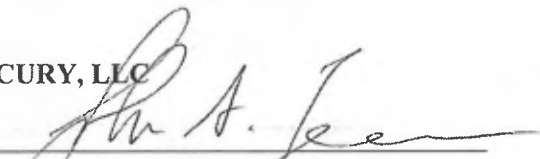
ISE GEMINI, LLC

By: 

Name: John Zecca

Title: SR. Vice President

ISE MERCURY, LLC

By: 

Name: John Zecca

Title: SR. Vice President

Investors' Exchange, LLC.

By: 

Name: John Schwall

Title: COO

Date: 10/3/16

ADDRESS FOR NOTICES:

Investors' Exchange, LLC.


4 World Trade Center, 44th Fl.

New York, NY 10037

Facsimile:

Attention: John Ramsay

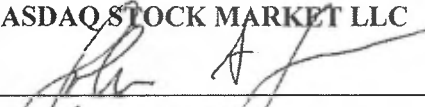
MIAMI INTERNATIONAL SECURITIES EXCHANGE LLC

By: 

Name: Edward Deitzel

Title: EVP, Chief Regulatory Officer & Chief Compliance Officer

THE NASDAQ STOCK MARKET LLC

By: 

Name: John Zecca

Title: SR. Vice President

NASDAQ BX, INC

By: 

Name: John Zecca

Title: SR. Vice President

NASDAQ PHLX LLC

By: _____

Name: _____

Title: _____

THE NASDAQ STOCK MARKET LLC

By: _____

Name: _____

Title: _____

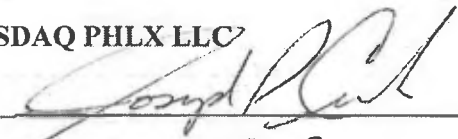
NASDAQ BX, INC.

By: _____

Name: _____

Title: _____

NASDAQ PHLX LLC

By:  _____

Name: Joseph P. Cusick

Title: VP. & CRO.

NATIONAL STOCK EXCHANGE, INC.

By: 

Name: James G. Buckley

Title: Chief Regulatory Officer


NYSE ARCA, INC.

By: 

Name: Elizabeth King

Title: General Counsel & Corporate Secretary


NEW YORK STOCK EXCHANGE LLC

By: 

Name: Elizabeth King

Title: General Counsel & Corporate Secretary

NYSE MKT LLC

By: 

Name: Elizabeth King

Title: General Counsel & Corporate Secretary

APPENDIX

Table of Contents

I.	SECURITY	5
A.	Industry Standards	5
B.	Data Encryption	5
C.	Cloud Security/FedRAMP Compliance.....	5
D.	Multifactor Authentication.....	6
E.	Internet Access to CAT.....	6
1.	Public Internet.....	6
2.	Use of Private Lines	6
F.	Partnerships with Other Organizations	6
G.	Penetration Testing	7
H.	Threat Monitoring.....	7
I.	Role of CISO.....	7
1.	Escalation.....	7
2.	Enforcement.....	7
3.	Imminent Security Threats.....	8
J.	End User Controls.....	8
1.	Policies and Procedures	8
2.	Memoranda of Understanding or Similar Agreements.....	8
K.	Personally Identifiable Information (“PII”)/Customer Information	8
1.	Definition of PII.....	8
2.	Usage of PII	9
L.	Bulk Data Extraction.....	10
1.	Regulatory Benefits	10
2.	Security of Extracted Bulk Data	11
II.	OTHER ITEMS	11
A.	Use of Legal Entity Identifier (“LEI”).....	11
B.	Customer Technical Specifications.....	12
C.	Symbology	13

D.	Existing Industry Messaging Protocols	13
E.	OATS Error Correction.....	13
F.	Clock Synchronization for Allocations.....	13
G.	Bidder Costs.....	14

I. SECURITY

A. Industry Standards

The Participants recognize the importance of protecting the security of the CAT, and, accordingly, the Participants believe it is critical that the CAT comply with relevant industry security standards at all times. As an initial matter, the Participants note that the CAT will be subject to the requirements of Regulation SCI, including applicable regulations regarding database security.³ In addition, at the outset of operation of the CAT, the Plan Processor will adopt all relevant standards from the NIST Cyber Security Framework, NIST 800.53 or ISO 27001 that would be appropriate to apply to the Plan Processor.⁴ Moreover, because industry standards may evolve over time, the Participants will require that the CAT's security program align with current industry standards and best practices as they evolve in the future. To this end, the Plan requires that the Plan Processor's information security program be reviewed at least annually by the Operating Committee.⁵

B. Data Encryption

Section 6.10(c)(ii) of the Plan requires, in part, that “[a]ll CAT Data returned shall be encrypted, and PII data shall be masked unless users have permission to view the CAT Data that has been requested.” Moreover, the Plan also requires that “[a]ll CAT Data must be encrypted in flight” and that “CAT Data stored in a public cloud must be encrypted at rest.”⁶ The Participants would like to reiterate that, given that all three remaining Bidders proposed cloud based solutions, all data will be encrypted in flight and at rest.

C. Cloud Security/FedRAMP Compliance

The Participants do not believe that the Plan Processor should be required to be certified pursuant to the Federal Risk and Authorization Management Program (“FedRAMP”). The Participants believe that requiring this certification could limit the portions of each cloud provider's solutions that each Bidder may access, while also increasing costs for the CAT. Furthermore, FedRAMP itself does not provide for additional security controls beyond that considered in the NIST standards, but rather focuses on providing a certification and evaluation process for government applications. Moreover, the Participants believe that the security controls required in the Plan and proposed by the Bidders, as well as those provided by the Bidders' cloud providers, are robust and would not be materially enhanced by requiring them to be FedRAMP certified. Additionally, regular third party audits, as required by the Plan, also would help to ensure the security of the CAT and any cloud solutions in use.⁷

³ See Plan, Section 6.9(b)(xi).

⁴ See Plan, Appendix D, Section 4.2 at Appendix D-14.

⁵ Plan, Section 6.12.

⁶ Plan, Appendix D, Section 4.1.2 at Appendix D-11.

⁷ See Plan, Appendix D, Section 4.1.3 at Appendix D-12.

D. Multifactor Authentication

Per the Participants' recent discussions with the SEC staff, the Participants note that the Plan, as proposed, requires that all logins be subject to multifactor authentication. Specifically, as stated in Appendix D, "MFA authentication capability for all logins (including non-PII) is required to be implemented by the Plan Processor."⁸

E. Internet Access to CAT

1. Public Internet

Under the Plan, and pursuant to the Bidders' solutions, the core CAT architecture would not be accessible via the public internet. Specifically, the Plan states that "[t]he CAT databases must be deployed within the network infrastructure so that they are not directly accessible from external end-user networks. If public cloud infrastructures are used, virtual private networking and firewalls/access control lists or equivalent controls such as private network segments or private tenant segmentation must be used to isolate CAT Data from unauthenticated public access."⁹

2. Use of Private Lines

The Plan does not require CAT Reporters to use private lines to connect to the CAT due to cost concerns, particularly for smaller broker dealers. Nevertheless, the Plan requires that CAT Reporters access the CAT via a secure, encrypted connection. Specifically, Appendix D states that "CAT Reporters must connect to the CAT infrastructure using secure methods such as private lines or (for smaller broker-dealers) Virtual Private Network connection over public lines."¹⁰

F. Partnerships with Other Organizations

The Plan requires the CAT LLC to "endeavor to join the [Financial Services Information Sharing and Analysis Center ("FS-ISAC")] and comparable bodies as the Operating Committee may determine."¹¹ The Participants do not intend to restrict partnerships only to FS-ISAC. Accordingly, the CAT LLC may seek to join other industry groups in addition to FS-ISAC as appropriate and as approved by the Operating Committee. For example, in addition to the FS-ISAC, the organizations that may be considered include National Cyber-Forensics & Training Alliance, the Department of Homeland Security's National Cybersecurity & Communications Integration Center, or other reputed cyber and information security alliances.

⁸ Plan, Appendix D, Section 4.1.4 at Appendix D-13.

⁹ Plan, Appendix D, Section 4.1.1. at Appendix D-11.

¹⁰ Plan, Appendix D, Section 4.1.1 at Appendix D-11.

¹¹ Plan, Section 6.5f(v).

G. Penetration Testing

The Plan requires the Plan Processor to perform penetration testing,¹² but provides flexibility as to when penetration testing would be conducted, including on an ad hoc or as necessary basis. For example, the Plan Processor may require penetration testing following major changes to system architecture (*e.g.*, changes in the network segmentation, major system upgrades, or installation of new management level applications), or identification of specific new threats that may necessitate testing.

H. Threat Monitoring

The Participants expect that the Plan Processor would adhere to industry practice for an infrastructure initiative such as the CAT, and, therefore, the Plan Processor would provide 24x7 operational monitoring, including monitoring and alerting for any potential security issues across the entire CAT environment. The three remaining Bidders have confirmed in their Bids that their proposed solutions provide for such 24x7, real time monitoring capabilities.

I. Role of CISO

1. Escalation

The Plan states that the Chief Information Security Officer (“CISO”) “shall be responsible for creating and enforcing appropriate policies, procedures, and control structures to monitor and address data security issues for the Plan Processor and the Central Repository.”¹³ In fulfilling such responsibilities, the CISO would be obligated to escalate certain issues that could represent a security threat to CAT Data.¹⁴ For example, if the CISO observes activity from a CAT Reporter or Participant that suggests that there may be a security threat to the Plan Processor or the Central Repository, then the CISO, in consultation with the Chief Compliance Officer, may escalate the matter to the Operating Committee. Notwithstanding the foregoing example, the Participants note that the details regarding such an escalation policy will not be determined until the Plan Processor has been selected.

2. Enforcement

The Plan requires the CISO to enforce appropriate policies, procedures and control structures related to security issues.¹⁵ The Participants do not envision, however, that such policy enforcement would involve a regulatory enforcement role with regard to the Participants. The Plan does not give the CISO the authority to engage in such regulatory enforcement. Moreover, although the Plan permits the Operating Committee to impose fees for late or inaccurate reporting of information to the CAT,¹⁶ it does not authorize the Participants to

¹² Plan, Section 6.2(b)(v)(H), and Appendix D, Section 4.1.3 at Appendix D-12.

¹³ Plan, Section 6.2(b)(v).

¹⁴ Plan, Appendix D, Section 4.1.4 at Appendix D-12.

¹⁵ Plan, Section 6.2(b)(v).

¹⁶ Plan, Section 11.3(c).

oversee, or serve enforcement actions against, each other via the Plan Processor. Only the SEC has such authority under the Securities Exchange Act of 1934.

3. Imminent Security Threats

As a part of its responsibility for data security, the CISO will be required to establish policies and procedures to address imminent security threats. Specifically, the Participants would expect the CISO to establish procedures for addressing security threats that require immediate action to prevent security threats to CAT Data. The details regarding such policies and procedures will be determined once the Plan Processor has been selected.

J. End User Controls

1. Policies and Procedures

The Plan requires the Participants to “establish, maintain and enforce written policies and procedures reasonably designed . . . to ensure the confidentiality of the CAT Data obtained from the Central Repository.”¹⁷ The Participants note that such policies and procedures will be subject to Regulation SCI and oversight by the SEC. Moreover, the Participants will consider all relevant standards from the NIST Cyber Security Framework, NIST 800.53 or ISO 27001 that would be appropriate to apply to such policies and procedures. In the event that relevant standards evolve, the proposed Plan also requires that “Each Participant shall periodically review the effectiveness of the policies and procedures . . . and take prompt action to remedy deficiencies in such policies and procedures.”¹⁸

2. Memoranda of Understanding or Similar Agreements

The Participants do not believe that memoranda of understanding (“MOUs”) or similar agreements between the CAT LLC and the Participants are necessary since the Participants will be bound by both their participation in the Plan as well as the agreement between the CAT LLC and the Plan Processor. However, the Participants believe that it is important that information regarding CAT Data usage, such as contact points and escalation procedures, be shared between the Plan Processor and the Participants, and, therefore, the Participants expect to establish such information sharing between the Plan Processor and the Participants once the Plan Processor is chosen. Moreover, the Participants expect that one of the CISO’s responsibilities would be to make sure that this information is captured and kept up to date appropriately.

K. Personally Identifiable Information (“PII”)/Customer Information

1. Definition of PII

The Participants believe that it would be helpful to clarify further the definition of PII as used throughout the Plan, including as used in Section 6.10(c) regarding the use of CAT Data by

¹⁷ Plan, Section 6.5(g).

¹⁸ Plan, Section 6.5(g).

regulators.¹⁹ The Plan defines and uses three categories of customer-related information: Customer Identifying Information, PII and Customer Account Information. “Customer Identifying Information” includes identifying information for both individuals and for entities, and is defined as:

information of sufficient detail to identify a Customer, including, but not limited to, (a) with respect to individuals: name, address, date of birth, individual tax payer identification number (“ITIN”)/social security number (“SSN”), individual’s role in the account (*e.g.*, primary holder, joint holder, guardian, trustee, person with the power of attorney); and (b) with respect to legal entities: name, address; Employer Identification Number (“EIN”)/Legal Entity Identifier (“LEI”) or other comparable common entity identifier, if applicable.²⁰

PII refers to personally identifiable information of individuals and includes social security number or tax identifier number or similar information.²¹ As such, the information covered by the terms PII and Customer Identifying Information include some of the same information. The term “Customer Account Information” is defined to include, subject to certain exceptions, account number, account type, customer type, date account opened, and large trader identifier (if applicable).²²

The Participants view all such customer-related information as highly sensitive information that requires the highest protections by the CAT and regulatory users of such information. Accordingly, all such customer-related information will be stored in a different, physically separated architecture, and will not be included in the result sets from online or direct query tools, reports or bulk data extraction related to the transactional CAT Data.²³ Instead, any queries, reports or extraction of the order/transactional CAT Data will only display identifiers, such as the Customer-ID, that do not convey PII, Customer Account Information or Customer Identifying Information. To unmask the customer-related information that corresponds to such identifiers, the regulatory user must be specifically authorized for such access.²⁴ The Participants recognize, however, that there is some inconsistency in how these terms are used in the Plan; accordingly, to the extent that any statement in the Plan, including Section 6.10(c), and Appendices C or D thereto, are inconsistent with the above description, the Participants recommend that the SEC amend the Plan accordingly.

2. Usage of PII

Section 6.10(c)(i)(B) of the Plan provides that “The user-defined direct queries and bulk extracts will provide authorized users with the ability to retrieve CAT Data via a query tool or language that allows users to query all available attributes and data sources.” The Participants

¹⁹ Section 6.10(c) of the Plan states that “PII data shall be masked unless users have permission to view the CAT Data that has been requested.”

²⁰ Plan, Section 1.1.

²¹ Plan, Section 1.1.

²² Plan, Section 1.1.

²³ Plan, Appendix D, Section 4.1.6 at Appendix D-14.

²⁴ Plan, Appendix D, Section 4.1.6 at Appendix D-14.

would like to clarify Section 6.10(c)(i)(B) with respect to the use of PII. In particular, the Participants note that customer-related information, including PII, will not be included in queries of the order/transactional database, nor will it be available in bulk extract form. Instead, the CAT will support the ability to query customer-related information, such as PII, stored in the separated architecture containing customer-related information. For example, if a regulatory user received a tip about a particular person, such user, if he or she were appropriately authorized to do so, could search the customer-related information database and view unmasked information to identify the person's Customer ID, and then use the Customer ID to query the order/transactional database to view relevant order and transactional activity for that Customer ID. Similarly, a regulatory user could access the customer-related information to identify persons in the same household as a named individual. In each such case, a regulatory user would have to be specifically authorized (via the process discussed in Section K.1, above) in order to access the database with customer-related information. The Participants expect the Plan Processor and the CISO to establish policies and procedures to identify abnormal usage of the database containing customer-related information, and to escalate concerns as necessary. The details regarding such policies and procedures will be determined once the Plan Processor has been selected.

L. Bulk Data Extraction

1. Regulatory Benefits

The Plan, as proposed, requires the Plan Processor to provide the regulators with the ability to perform bulk data extracts.²⁵ The Participants continue to believe that permitting regulators to extract order/transaction data from the Central Repository for regulatory use (*i.e.*, "bulk data extracts") is important for their regulatory purposes, and that eliminating or limiting bulk data extracts of the CAT Data may significantly and adversely impact the Participants' ability to effectively surveil their markets using CAT Data.²⁶ As noted in the Plan, the Participants currently plan to enrich existing surveillances using bulk data extracts of CAT Data. For example, as the Plan notes, "[t]he bulk extract feature will replace the current Intermarket Surveillance Group (ISG) ECAT and COATS compliance data files that are currently processed and provided to Participants for use in surveillance applications. These files are used extensively across all Participants in a variety of surveillance applications and are a critical data input to many surveillance algorithms."²⁷ Removing the ability to extract data from the CAT could limit the usefulness of CAT Data to the Participants.

²⁵ Plan, Section 6.10(c); and Appendix D, Section 8.2 at Appendix D-29.

²⁶ However, as discussed in Section K.2, above, customer-related information, including PII, will not be included in queries of the order/transactional database, nor will it be available in bulk extract form.

²⁷ Plan, Appendix D, Section 8.2 at Appendix D-29. The Plan notes that "[t]he bulk extract feature will replace the current Intermarket Surveillance Group (ISG) ECAT and COATS compliance data files that are currently processed and provided to Participants for use in surveillance applications. These files are used extensively across all Participants in variety of surveillance applications and are a critical data input to many surveillance algorithms."

2. Security of Extracted Bulk Data

The Participants recognize the security concerns raised by bulk data extracts and any Participant-controlled systems (*e.g.*, Participant sandboxes residing in the Plan Processor's cloud or a Participant's local system) used to store and analyze such data extracts, but believe that requiring the Participants to adopt and enforce policies and procedures to address these security issues appropriately addresses these concerns without diminishing the surveillance benefits of the CAT. The Plan requires the Participants to "establish, maintain and enforce written policies and procedures reasonably designed . . . to ensure the confidentiality of the CAT Data obtained from the Central Repository."²⁸ Accordingly, the Plan requires Participants to have policies and procedures reasonably designed to ensure the confidentiality of CAT Data obtained through bulk data extracts and maintained in the Participants' systems. The Participants' own security controls, not those of the Plan Processor, would apply to such systems as they would be outside the Plan Processor's control. The Participants' security controls would be consistent with industry standards, including security protocols that are compliant with Regulation SCI, and the Participants would periodically review the effectiveness of such controls pursuant to their policies and procedures addressing data security. The Plan Processor's security controls, however, would apply to all aspects within its control. For example, as stated in the Plan, "[e]xtraction of data must be consistently in line with all permissioning rights granted by the Plan Processor. Data returned must be encrypted, password protected and sent via secure methods of transmission."²⁹ Moreover, the Plan Processor's information security program will be subject, at least annually, to the Operating Committee's review and approval, in accordance with the proposed Plan.³⁰

II. OTHER ITEMS

A. Use of Legal Entity Identifier ("LEI")

In the September 23rd Letter, the Participants stated that it would be reasonable to require an Industry Member to provide its LEI or the LEI of a customer to the CAT as part of Customer Identifying Information if the Industry Member has or acquires such LEI, rather than specifically requiring that Industry Members or others obtain LEIs if they do not already have them. After additional consideration, the Participants would like to clarify that Industry Members that provide LEIs to the CAT would provide such LEIs in addition to, rather than in lieu of, other Customer Identifying Information. Accordingly, the Participants recommend that the SEC amend the definition of Customer Identifying Information as set forth in Section 1.1 of the Plan – and that such amendment shall supersede and replace the amendment set forth in the September 23rd Letter – as follows:

"Customer Identifying Information" means information of sufficient detail to identify a Customer, including, but not limited to, (a) with respect to individuals: name, address, date of birth, individual tax payer identification number ("ITIN")/social security number

²⁸ Plan, Section 6.5(g).

²⁹ Plan, Appendix D, Section 8.2.2 at Appendix D-31.

³⁰ See, *e.g.*, Plan, Section 6.12; Plan, Appendix D, Section 4 at Appendix D-10 ("Data Security").

(“SSN”), individual’s role in the account (*e.g.*, primary holder, joint holder, guardian, trustee, person with the power of attorney); and (b) with respect to legal entities: name, address, Employer Identification Number (“EIN”)/LEI or other comparable common entity identifier, if applicable; provided, however, that an Industry Member that has an LEI must submit its LEI, and where the LEI or other common entity identifier is provided, such LEI or other common entity identifier would be provided in addition to, not in lieu of, information covered by such LEI or common entity identifier (*e.g.*, name, address)[would not need to be separately submitted to the Central Repository].

[additions underlined; deletions bracketed]

The Participants also would like to extend a similar requirement to Participants reporting to the CAT. Therefore, the Participants should provide to the CAT any LEIs used by Industry Members, to the extent that the Participants already have or acquire such LEIs, and without the imposition of any due diligence obligations beyond those that may exist today with respect to information associated with an LEI, when making daily submissions in accordance with Section 6.3(e)(i). Accordingly, the Participants recommend that the SEC amend Section 6.3(e)(i) of the Plan to state:

- (i) Each Participant must submit, on a daily basis,
 - (A) all SRO-Assigned Market Participant Identifiers used by its Industry Members or itself; and[as well as]
 - (B) information to identify the corresponding market participant (*e.g.*, CRD number, or LEI) to the Central Repository; provided, however, if the Participant has the LEI for an Industry Member, the Participant must submit the LEI of such Industry Member.

As described in Section 6.3(e)(i), such LEIs would be reported to the CAT in addition to, rather than in lieu of, SRO-Assigned Market Participant Identifiers (that is, “an identifier assigned to an Industry Member by an SRO or an identifier used by a Participant,”³¹ such as an MPID). Accordingly, if an Industry Member has an LEI, the Participant would submit both the SRO-Assigned Participant Identifier and the LEI.

B. Customer Technical Specifications

The Plan, as supplemented by the September 23rd Letter, sets forth various milestones for the publication and implementation of the methods for providing information to the Customer-ID Database and the submission of order and market maker quote data to the Central Repository.³² In particular, the proposed timeline for the Plan Processor to publish Technical Specifications for Industry Members to report Customer Account Information to the Central Repository (six months) differs from the proposed timeline for the Plan Processor to publish

³¹ Plan, Section 1.1.

³² Plan, Appendix C, Section C.10 at Appendix C-99 – C-102.

Technical Specifications for Industry Member submission of order data (one year). The Participants recognize that reporting order data to the CAT will be a significantly more complex process than reporting Customer Account Information and, accordingly, believe that it is appropriate to allow Industry Members more time to review Technical Specifications and to begin testing their systems with regard to order data.

C. Symbology

The Participants would like to clarify further the discussion of symbology that was included in the September 23rd Letter. In the September 23rd Letter, the Participants stated that “[b]ased on discussions with the DAG, the Participants understand that all Industry Members subject to OATS or electronic blue sheet reporting requirements currently use the symbology of the listing exchange when submitting such reports.” The Participants would like to add that, based on their understanding of current practices, Industry Members currently employ technical solutions and/or systems that allow them to translate symbology into the correct format of the listing exchange when submitting data to exchanges or when submitting to regulatory reporting systems such as OATS or electronic blue sheets.

D. Existing Industry Messaging Protocols

The Participants believe that the nature of the data ingestion is key to the architecture of the CAT, and, therefore, the Plan does not mandate the data ingestion format for the CAT.³³ However, the Bids of the three remaining Bidders propose accepting existing messaging protocols (e.g., FIX), rather than requiring CAT Reporters to use a new format.

E. OATS Error Correction

To facilitate the Commission’s review of the Plan, the Participants would like to provide additional information on the correction of errors in OATS reporting. Based on a review of OATS data from August 2016, FINRA has determined that the majority of errors reported to OATS were corrected within six business days of submission (approximately 91.26% of error corrections), with most corrections occurring on two days. Specifically, 26.46% of error corrections occurred one day after submission,³⁴ and 59.45% of error corrections occurred six days after submission, or five days after final rejection feedback becomes available, which is the OATS rejection repair deadline.³⁵

F. Clock Synchronization for Allocations

In the September 6th Letter, the Participants stated that they “propose to amend the Plan to permit CAT Reporters to report the time for Allocation Reports with a granularity of one

³³ Plan, Appendix C, Section 12(f) at Appendix C-122.

³⁴ Note that syntax rejections are available within four hours of submission.

³⁵ Additionally, approximately 0.48% of error corrections were made on the day of submission, approximately 4.86% of error corrections were made two to five days after submission, and the remaining approximately 8.75% of error corrections were made seven to 36 days after submission.

second (as it is for Manual Order Events).” The Participants also believe that the Plan should be amended to permit Industry Members to synchronize their Business Clocks used solely for reporting of the time of allocation on Allocation Reports to within one second. Accordingly, the Participants recommend that the SEC amend the Plan by adding new Section 6.8(a)(iv) as follows:

(iv) through its Compliance Rule, require its Industry Members to synchronize their Business Clocks used solely for the time of allocation on Allocation Reports at a minimum to within one second of the time maintained by the NIST, consistent with industry standards, and maintain such synchronization. Each Participant shall require its Industry Members to certify periodically (according to a schedule defined by the Operating Committee) that their Business Clocks used solely for the time of allocation on Allocation Reports meet the requirements of the Compliance Rule. The Compliance Rule of a Participant shall require its Industry Members using Business Clocks solely for the time of allocation on Allocation Reports to report to the Plan Processor any violation of the Compliance Rule pursuant to the thresholds set by the Operating Committee.

The Participants further recommend that the SEC amend Section 6.8(a)(i) of the Plan to incorporate corresponding changes as follows:

(a) Each Participant shall:

(i) other than such Business Clocks used solely for Manual Order Events, synchronize its Business Clocks at a minimum to within 50 milliseconds of the time maintained by the National Institute of Standards and Technology, consistent with industry standards;

(ii) other than such Business Clocks used solely for Manual Order Events or the time of allocation on Allocation Reports, through its Compliance Rule, require its Industry Members to:

(A) synchronize their respective Business Clocks at a minimum to within fifty (50) milliseconds of the time maintained by the National Institute of Standards and Technology, and maintain such a synchronization;

* * * * *

[Additions underlined; deletions bracketed]

G. Bidder Costs

As noted in the September 23rd Letter, pursuant to recent discussion with and submissions by the Bidders, the Bidders indicate that the expected Plan Processor costs are less than originally proposed, now ranging from approximately \$37.5 - \$65 million for building the

CAT and approximately \$36.5 - \$55 million for annual operations.³⁶ The Participants note that these are only estimates and the final costs may differ. In particular, because these estimates are based on requirements in the proposed Plan; any additional requirements in the approved Plan, including those suggested by the Participants in this and prior letters to the SEC, could impact costs. In addition, these estimates do not include additional CAT expenses that may be incurred, such as for insurance, operating reserves, or third party costs such as accounting and legal.

³⁶ September 23rd Letter at 11, n.30.