July 15, 2016

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

Marcia E. Asquith
Corporate Secretary
Office of the Corporate Secretary
Financial Industry Regulatory Authority
1735 K Street, NW
Washington, DC 20006-1506

Re: Joint Industry Plan; Notice of Filing of the National Market System Plan Governing the Consolidated Audit Trail ("CAT"), File Number 4-698

Dear Mr. Fields and Ms. Asquith:

The Financial Services Roundtable[1] ("FSR") respectfully submits this letter in support of the CAT proposal[2] (the "Proposal") to implement a national market system plan (the "CAT Plan") to comply with SEC Rule 613 of Regulation NMS.[3] The self-regulatory organizations (the "SROs") have filed an amendment to the CAT Plan which is incorporated into the Proposal.

---

1 As *advocates for a strong financial future*™, FSR represents the largest integrated financial services companies providing banking, insurance, payment and investment products and services to the American consumer. Member companies participate through the Chief Executive Officer and other senior executives nominated by the CEO. FSR member companies provide fuel for America's economic engine, accounting directly for $92.7 trillion in managed assets, $1.2 trillion in revenue, and 2.3 million jobs.

2 Joint Industry Plan; Notice of Filing of the National Market System Plan Governing the Consolidated Audit Trail, Securities and Exchange Commission Release No. 34-77724; File No. 4-698 (Apr. 27, 2016), available at https://www.sec.gov/rules/sro/nms/2016/34-77724.pdf.

3 17 C.F.R. § 242.163.

As discussed in more detail below, FSR supports the development of the CAT Plan. We do, however, have several concerns with the CAT Plan in its current form. We believe that the CAT Plan can be implemented in a manner that could address some of the industry's concerns while providing the benefits to the Securities and Exchange Commission ("SEC") and the Participants[4] as contemplated by the Proposal.

While FSR supports the CAT Plan, this comment letter addresses key concerns related to certain aspects of its proposed structure and implementation. The significant issues are as follows:

- *Data Access and Privacy:* The CAT Plan should incorporate adequate CAT Data access controls and allow Industry Members[5] to review specific controls designed by the selected Plan Processor. Further, Industry Members have cybersecurity breach concerns, including the cost of insurance coverage for such incidents. FSR proposes that CAT NMS LLC purchase an insurance policy that covers potential breaches and extends to the Industry Members.

- *Reporting Accuracy:* The FSR supports uniform clock synchronization across all trade reporting systems and agrees with the proposed error rate phased-down approach.

- *Expense:* Industry Members are concerned about the cost of the CAT Plan and its impact on investors. Costs may be reduced by decommissioning current reporting systems simultaneously with implementation of the CAT Plan to avoid duplicative reporting requirements and costs.

- *Timetable:* FSR proposes an acceleration of the Plan Processor selection process, synchronization of retirement and implementation of all reporting systems, and a six- to twelve-month extension of the CAT Plan

---

[4] "Participant" means BATS Exchange, Inc.; BATS Y-Exchange, Inc.; BOX Options Exchange LLC; C2 Options Exchange, Incorporated; Chicago Board Options Exchange, Incorporated; Chicago Stock Exchange, Inc.; EDGA Exchange, Inc.; EDGX Exchange, Inc.; Financial Industry Regulatory Authority, Inc.; ISE Gemini, LLC; International Securities Exchange, LLC; Miami International Exchange LLC; NASDAQ OMX BX, Inc.; NASDAQ OMX PHLX LLC; The NASDAQ Stock Market LLC; National Stock Exchange, Inc.; New York Stock Exchange LLC; NYSE MKT LLC; NYSE Arca, Inc; and any Person that becomes a Participant as permitted by the Limited Liability Company Agreement of CAT NMS, LLC, in such Person's capacity as a Participant in the Company (it being understood that the Participants shall comprise "members" of the Company (as the term "member" is defined in Section 18-101(11) of the Delaware Limited Liability Company Act.

[5] "Industry Member" means "a member of a national securities exchange or a member of a national securities association." *See* Section 1.1 of the CAT NMS Plan.

implementation timetable to allow Industry Members to comply with other significant regulatory changes, including the Department of Labor's fiduciary duty regulation[6] as well as the T+2 implementation.

FSR greatly appreciates the opportunity to comment on the Proposal. For ease of reference, we have reproduced in bold typeface a selection of requests for comment from the Proposal, followed by our response in plain text.

Data Access

1. *Cybersecurity*

a. *Personally Identifiable Information*

Do Commenters believe that the CAT NMS Plan adequately addresses the protection and security of Personally Identifiable Information in CAT?[7]

The CAT Plan provides a list of the data points that need to be reported for each Reportable Event,[8] including customer identification information, which may include Personally Identifiable Information ("PII"). Currently, PII is collected by Industry Members, but is not reported to Participants, except during an inquiry or examination or pursuant to a subpoena; this will be a big change for the industry and raises significant data security and privacy concerns. Upon commencement of reporting, Industry Members must submit an initial set of customer information (including PII) and update that information on a daily basis thereafter. The Participants will select a Plan Processor[9] that will be responsible for the security of the Central Repository.[10]

---

6 *See* Definition of the Term "Fiduciary"; Conflict of Interest Rule—Retirement Investment Advice, 81 Fed. Reg. 20,946 (Apr. 8, 2016).

7 *See* Proposal, *supra* note 2 at p. 173.

8 "Reportable Event" means "includ[ing],but…not limited to, the original receipt or origination, modification, cancellation, routing, execution (in whole or in part) and allocation of an order, and receipt of a routed order." *See* Section 1.1 of the CAT NMS Plan.

9 As set forth in Section 1.1 of the CAT NMS Plan, the Plan Processor "means the Initial Plan Processor or any other Person selected by the Operating Committee pursuant to SEC Rule 613 and Sections 4.3(b)(i) and 6.1, and with regard to the Initial Plan Processor, the Selection Plan, to perform the CAT processing functions required by SEC Rule 613 and set forth in [the CAT NMS Plan]."

10 The CAT NMS Plan defines "Central Repository" as "the repository responsible for the receipt, consolidation, and retention of all information reported to the CAT pursuant to SEC Rule 613 and [the Limited Liability Company Agreement of CAT NMS, LLC]."

Given the industry's recent focus on cybersecurity, the SEC and Participants should consider security measures related to the CAT Data. The Proposal discusses several alternatives for the security of the CAT Data especially surrounding PII. As discussed in the Proposal, the PII security should be encrypted both "in-transit" and "at-rest," and stored in a separate location from other CAT Data. In addition, the extraction of all CAT Data returned will be encrypted, and PII data will be masked unless users have permission to view the PII contained in the CAT Data that has been requested.[11] Because the security measures may vary depending on which Plan Processor is selected, we urge the SEC, Operating Committee, and Participants to vet each Plan Processor's proposal regarding PII security.

Due to the sensitivity of CAT Data, and recent high profile data breaches hitting both public and private sector entities,[12] steps must be taken to ensure proper controls are in place to protect the data throughout its lifecycle using secure, authenticated and

---

11 *See* Proposal, *supra* note 2 at p. 75.

12 *See, e.g.*, Gregory C. Wilshusen, Director, Information Security Issues, *Information Security: Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies*, Testimony Before the Subcommittees on Research and Technology and Oversight Committee on Science, Space, and Technology, House of Representatives, GAO-15-758T at 2 (July 8, 2015) (finding that concerns about cyber-based threats to federal systems "are further highlighted by recent incidents involving breaches of sensitive data and the sharp increase in information security incidents reported by federal agencies over the last several years, which have risen from 5,503 in fiscal year 2006 to 67,169 in fiscal year 2014"), *available at* http://www.gao.gov/assets/680/671253.pdf; Gregory C. Wilshusen, Director, Information Security Issues, *Cybersecurity: Recent Data Breaches Illustrate Need for Strong Controls across Federal Agencies*, Testimony Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of Representatives, GAO-15-725T (June 24, 2015) (warning that "[until] federal agencies take actions to address these challenges—including implementing the hundreds of recommendations we and inspectors general have made—federal systems and information will be at an increased risk of compromise from cyber-based attacks and other threats), *available at* http://www.gao.gov/assets/680/670935.pdf; GOVERNMENT ACCOUNTABILITY OFFICE, *High-Risk Series: An Update*, GAO-15-290 at 236 (Feb. 2015) (finding that the "number of reported security incidents involving [personally identifiable information] at federal agencies has increased dramatically in recent years"), *available at* http://www.gao.gov/assets/670/668415.pdf. *See also*, Cory Bennett, *OPM hack hit over 22 million people*, THE HILL (July 9, 2015) (reporting that "more than 22 million people have had their personal information stolen" from the U.S. Office of Personnel Management), *available at* http://thehill.com/policy/cybersecurity/247410-report-opm-hack-hit-over-25-million-people; Patrick Zengerle and Megan Cassella, *Millions more of Americans hit by a government personnel data hack*," REUTERS (July 9, 2015), *available at http://www.reuters.com/article/2015/07/09/cybersecurity-usa-idUSKCN0PJ2MQ20150709;* Chris Strohm, *U.S. Hack May Have Disclosed 18 million Social Security Numbers*, BLOOMBERG BUSINESS (June 24, 2015) (reporting that the "agency that manages U.S. government personnel records is investigating whether Social Security numbers for as many as 18 million people were taken in the massive cyber-attack"), *available at* http://www.bloomberg.com/news/articles/2015-06-24/u-s-hack-may-have-disclosed-18-million-social-security-numbers.

industry-accepted encryption mechanisms. As the Government Accountability Office (the "GAO") notes, "the ineffective protection of cyber assets can result in the loss or unauthorized disclosure or alteration of information, [which] could lead to serious consequences and result in substantial harm to individuals and to the federal government."[13] The GAO further noted technological advances have enabled individuals and organizations "to correlate [personally identifiable information] and track it across large and numerous databases."[14]

Controls protecting the data should consider the risk of state-backed threat actors, outside criminal elements and potential insider threats. Persons with authorized access to the data should have comprehensive background checks at the time of hire and these background checks should be performed continuously, on a periodic basis, to avoid insider threat concerns. As described in the Proposal, FSR agrees that the Plan Processor should implement authorized user access controls; including high-level criteria (*i.e.*, "need-to-know") surrounding authorized user access to PII.

We recommend the following standards to protect the three states of CAT Data:

I. In-Transit Data. Data in-transit across networks, to include client-to-server, server-to-server communication, as well as any data transfer between CAT Data systems and authorized third-party systems, must be protected with asymmetric encryption. Transport Layer Security using version 1.2 or newer versions of the protocol to safeguard against eavesdropping and ensure the integrity of the data should be considered. Known weak cipher suites such as 3DES, RC4, and SHA must be avoided. An example of a currently known good cipher suite is ECDHE-RSA-AES256-GCM-SHA384.

II. Data At-Rest. Data at-rest should be protected by similar encryption practices; however, symmetric encryption may be considered in concert with other controls leveraging industry best practices for key management such as those defined in the most recent version of NIST Special Publication 800-57. Special care should be taken in the generation and storage of cryptographic keys to ensure the data is protected from unauthorized access. The data itself should be segmented and isolated from general use networks and systems and the Plan Processor must adhere to a policy of "least privilege".

III. Data In-Use. Data in-use, such as decrypted or copied data, should have data protection controls in place. For example, if data is provided to

---

[13] GOVERNMENT ACCOUNTABILITY OFFICE, *High-Risk Series: An Update*, GAO-15-290 at 235 (Feb. 2015).

[14] *Id.*

> authorized users (*e.g.*, the SEC or Participants), then the authorized users must disclose their intended use of the data and for how long. Once the data is no longer needed, the authorized user must demonstrate that it has disposed of the data in a way that prevents recovery and should certify that the data has been destroyed. NIST Special Publication 808-88 may be used as a reference for proper disposal and sanitization techniques.

In addition, the PII must be made available on a "need to know basis" to the SEC and Participants, as well as to Industry Members for error correction. Further, the technical specification of the CAT Plan provides that the Plan Processor design the technology associated with the CAT Plan to, at a minimum, satisfy all applicable regulations regarding database security, including provisions of Regulation Systems Compliance and Integrity under the Securities Exchange Act of 1934 ("Reg SCI").[15] The Plan Processer should ensure access to the PII complies with Reg SCI, and any other applicable federal and state privacy laws (collectively, "Privacy Laws"). The Operating Committee, along with the Participants, must develop policies and procedures to comply with the Privacy Laws and require the Plan Processor and Service Providers[16] to abide by such requirements. However, the CAT Plan should not expand the scope of the Privacy Laws applicable to Industry Members. The Industry Members are subject to certain applicable federal and state privacy laws, but are not currently required to comply with Reg SCI. The CAT Plan should make clear that Reg SCI would not be expanded to apply to an Industry Members by virtue of its reporting requirements under the CAT Plan. Moreover, FSR believes that the Operating Committee should develop reporting procedures that would require prompt notice to Industry Members of any CAT Data security breach.

Finally, the Proposal does not provide enough granularity related to actual controls, service levels, and technical support that will be implemented by the Plan Processor. For example, Industry Members need to know what service levels and liability will be associated with data transfers between CAT Reporters and the CAT Processor. Industry Members also need to know how information security will be addressed with customer service staff at the Plan Processor to assist CAT Reporters with troubleshooting. Although the Proposal gives the Plan Processor the flexibility to implement its own procedures to comply with the CAT Plan, Industry Members should be given the opportunity to review and comment on the specific requirements proposed by the Plan Processor.

---

15 *See* Proposal, *supra* note 2 at p. 70.

16 *See* Proposal, *supra* note 2 at p. 45 (requiring the Plan Processor to enter into service level agreements with service providers to govern performance of the Central Repository).

b. *Breach and Insurance*

Do Commenters believe that the CAT NMS Plan appropriately allocates responsibility for the security and confidentiality of CAT Data among the Participants, the Plan Processor and other parties?[17]

In recent years, targeted cybersecurity attacks in the financial services industry are on the rise. Hackers are becoming smarter, developing new technology, and finding ways to penetrate complex technology and security systems at major financial institutions and regulatory agencies. The industry has developed strong controls to protect their confidential information, including PII, but the security concerns are an on-going issue that must be continuously reviewed and revised in light of recent cybersecurity attacks and breaches.

The CAT Plan provides a strong foundation to protect against cybersecurity breaches, including the appointment of a Chief Information Security Officer ("CISO") who is responsible for creating and enforcing policies to monitor and address data security issues, including connectivity, encryption, breach management, data storage, PII data requirements, and penetration testing. The Plan Processor will also need to develop Data Loss Prevention, Business Continuity, and Cyber Incident Response plans.

Developing policies and procedures is an important step towards the protection against security breaches, but the Operating Committee needs to be vigilant about evaluating each policy developed by the CISO or Plan Processor, along with results from the penetration testing, to ensure that the CAT Plan is prepared for a cybersecurity incident.

The Proposal discusses the economic analysis related to the implementation and maintenance of the CAT Plan, along with potential costs of a security breach. However, an accurate cost estimate of a cyber-attack is difficult to quantify, along with reputational damage that may ensue. In addition, the Proposal fails to address who is responsible for the cost of the breach that occurs at the Central Repository. Ultimately, the Industry Members are likely to be subject to liability by the investors for the cyber-attack and misappropriation of an investor's PII. However, the Industry Members have no control over the security measures of the Plan Processor with respect to the CAT Data stored in the Central Repository or "in-transit" amongst the SEC and Participants.

In addition, the CAT Data could be exported to the technology systems of the SEC or Participants, which are not subject to the security standards as outlined in the Proposal or developed by the Plan Processor (although the Participants are required to comply with Reg SCI). To mitigate some of these risks, the CAT Plan should prohibit the export of PII once it is submitted by Industry Members and stored in the Central

[17] *See* Proposal, *supra* note 2 at p. 170.

Repository. All analytics of CAT Data should be run through the Plan Processor at the Central Repository.

Industry Members should not bear the costs of a security breach that occurs on the systems of the SEC, the Participants, Plan Processor, Central Repository, or "in-transit" amongst the various parties. The cost of complying with the notification requirements under the Privacy Laws may be exorbitant and should not be the responsibility of Industry Members who have no control over these systems or security measures surrounding these systems.

We propose that CAT NMS LLC purchase an insurance policy that covers all of these potential breaches and extends to the Industry Members and their obligations *vis-à-vis* their clients whose CAT Data is required to be reported by the CAT Plan. The cost of the insurance policy may be allocated amongst the various Industry Members, but would be at a lower cost than holding each Industry Member responsible for a potential breach related to the CAT Plan.

Reporting Accuracy

1. *Clock Synchronization:*

Do Commenters believe that a clock offset tolerance of 50 milliseconds is appropriate and reasonable, in light of the increase in the speed of trading over the last several years? If not, what would an appropriate and reasonable standard be?[18]

One stated purpose of the CAT Plan is to enable regulators to more easily identify sources of market disruptions during events like the 2010 "flash crash." The CAT Plan will require Participants and Industry Members to synchronize business clocks, except those used solely for manual orders, to within 50 milliseconds of the time maintained by the National Institute of Standards and Technology. The SEC proposed this increment based on industry feedback and balancing cost versus accuracy. Given that FINRA has already established requirements for complying with clock synchronization tolerances, we recommend that the CAT Plan adhere to the existing FINRA policies on clock synchronization, currently at 50 milliseconds. FSR supports one uniform clock synchronization standard across the broad broker-dealer community in an effort to avoid unnecessary market segmentation.

We note that the Operating Committee has the ability to revise the synchronization and time stamp requirement at any time. As such, we urge the Commission and Participants to consider making any proposed changes prior to the

[18] *See* Proposal, *supra* note 2 at p. 111.

effective date in order to reduce the cost of adapting the technology after implementation to comply with a revised synchronization requirement.

Further, FSR recommends that the Proposal be revised to remove the time stamp requirement for allocations. Allocations are performed on a post-trade basis and are not time critical. Further, an obligation to implement technology for time stamps on allocations will require Industry Member to incur an unnecessary cost of additional resources that would be better served implementing other critical requirements of the CAT Plan.

2. *Error Rate:*

Do Commenters believe that CAT NMS Plan's initial maximum Error Rate of 5% for CAT Data reported to the Central Repository is appropriate in light of OATS' current error rate of less than 1%?[19]

The CAT Plan permits an initial error rate of 5% for reporting, which will be phased down to 1% over a four-year period. The 5% was based on the industry's experience with an initial 5% error rate for OATS reporting, which is currently less than 1%. FSR agrees with the Proposal, but believes that this error rate should be applied post-correction, not pre-correction as stated in the CAT Plan, and that it should only apply to equities reporting.

Expense

1. Do Commenters agree with the SEC's analysis of the Plan's funding model? Why or why not? Are there additional factors that should be considered?[20]

The Proposal provides an extensive discussion on the economic analysis related to the costs associated with the implementation of the CAT Plan, the on-going maintenance of the CAT Plan, and costs to the Industry Members and the ultimate investor. The total cost is estimated to be in excess of $3 billion. The discussion includes estimates from each Plan Processor who submitted a bid for the project, as well as surveys from a variety of Industry Members. Further, the analysis discusses the costs of decommissioning existing reporting systems, along with the cost savings for eliminating such systems. However, the overarching theme throughout the analysis is that these estimates may not be an accurate reflection of actual costs.

Moreover, the Proposal does not adequately explain what is included in the calculation of "costs" of the system, nor is it entirely clear who will bear such costs. What is clear is that the ultimate cost will be in the billions, which will be passed-down to the

---

19 *See* the Proposal, *supra* note 2 at p. 153.

20 *See* the Proposal, *supra* note 2 at p. 516.

Industry Members and investors through new fees. However, FSR believes it is important for the SEC and the Participants to be allocated some of the costs, given that the CAT Plan provides a benefit directly to the regulators as a resource for regulatory oversight and surveillance capabilities.

Decommissioning of Current Reporting Systems

It is important that the current reporting systems (*e.g.*, OATS reporting) be decommissioned as quickly as possible in an effort to reduce the cost and administrative burden on Industry Members. To the extent that any subset of data collected under the CAT Plan is otherwise collected under a different reporting regime, the existing reporting regime should be amended as soon as possible to remove the duplicative reporting requirement.

Timetable

The CAT Plan provides a detailed implementation schedule, all of which will happen within three years of the effective date. FSR believes the timeline must be extended in order to provide the industry a sufficient amount of time to comply with the new reporting structure under the CAT Plan, including the ability to report CAT Data in a timely and accurate manner with a reduced error rate, as discussed above. FSR believes the release of final technical specifications should drive the implementation timeline. A review of the technical specifications is necessary in order to accurately estimate the effort involved in implementing CAT functionality. Industry Members should be provided a copy of the technical specifications and given an opportunity to review and provide feedback to the Plan Processor in an effort to determine an appropriate implementation schedule. As such, FSR recommends the acceleration of the Plan Processor selection process.

FSR believes the launch of the CAT Plan should be linked to the retirement of existing reporting systems. Specifically, FSR recommends replacing the currently contemplated duplicative reporting period with a test period of the new CAT reporting system. It is important to maintain a single audit trail of record (*i.e.*, for only one reporting system to be in place at any one time) to avoid duplicative reporting.

At a minimum, FSR suggests the implementation be extended for a period of at least six to twelve months beyond the timeframe currently proposed, particularly in light of the fact that many Industry Members will be working to comply with the Department of Labor's new fiduciary duty regulation as well as T+2 implementation during this same timeframe. The extended timetable will provide the Industry Members with additional time to decommission current reporting systems to coincide with the implementation of the new system. The extended implementation timetable would also allow for additional testing and synchronization, which will result in a more accurate reporting environment on "go-live" date. As discussed in the Proposal, the Industry Members may incur

additional costs by operating two separate reporting systems. Therefore, the ability to combine the various technology and regulatory projects may provide some additional cost savings.

* * *

FSR appreciates the opportunity to submit comments on the CAT Plan. If it would be helpful to discuss FSR's specific comments or general views on this issue, please contact me at [redacted], or Felicia Smith, Vice President and Senior Counsel for Regulatory Affairs at [redacted].

Sincerely yours,

Richard Foster
Senior Vice President and Senior Counsel
for Regulatory and Legal Affairs
Financial Services Roundtable

With a copy to:

The Honorable Mary Jo White, Chair
The Honorable Kara M. Stein
The Honorable Michael S. Piwowar
Members*, United States Securities and Exchange Commission*

Stephen Luparello, Director, Division of Trading and Markets
United States Securities and Exchange Commission