MANAGED FUNDS ASSOCIATION
The Voice of the Global Alternative Investment Industry
WASHINGTON, DC | NEW YORK

July 18, 2016

Via Website Submission

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

Re: File No. 4-698; Consolidated Audit Trail

Dear Mr. Fields:

Managed Funds Association[1] ("**MFA**") appreciates the opportunity to submit comments to the Securities and Exchange Commission (the "**Commission**" or "**SEC**") on its Notice of Filing of the National Market System ("**NMS**") Plan Governing the Consolidated Audit Trail by NMS Plan participants (the "**CAT NMS Plan**").[2] MFA supports the Commission and the NMS Plan Participants' goal of modernizing the regulatory data infrastructure upon which regulators rely for overseeing the markets. The CAT NMS Plan is an extensive undertaking, which if finalized and executed appropriately, will introduce a powerful order tracking tool that will be critical to the Commission's market oversight infrastructure for decades to come. Due to the scale and importance of the information gathered and housed in the Consolidated Audit Trail, the CAT NMS Plan also creates serious new vulnerabilities for market participants, the markets, and even national

[1] Managed Funds Association ("**MFA**") represents the global alternative investment industry and its investors by advocating for sound industry practices and public policies that foster efficient, transparent, and fair capital markets. MFA, based in Washington, DC, is an advocacy, education, and communications organization established to enable hedge fund and managed futures firms in the alternative investment industry to participate in public policy discourse, share best practices and learn from peers, and communicate the industry's contributions to the global economy. MFA members help pension plans, university endowments, charitable organizations, qualified individuals and other institutional investors to diversify their investments, manage risk, and generate attractive returns. MFA has cultivated a global membership and actively engages with regulators and policy makers in Asia, Europe, North and South America, and many other regions where MFA members are market participants.

[2] SEC Release No. 34-77724 (Apr. 27, 2016) (hereinafter, the "**Notice**"), available at: https://www.sec.gov/rules/sro/nms/2016/34-77724.pdf. The NMS Plan participants are: 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., International Securities Exchange, LLC, ISE Gemini, LLC, Miami International Securities 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, and NYSE Arca, Inc. (hereinafter, the "**NMS Plan Participants**").

security. As Chair White recently noted, the CAT is a "very complex undertaking that must be done carefully and correctly."[3]

In the intervening years since the Consolidated Audit Trail was first proposed, cybersecurity has become a much more serious concern. As we discuss in more detail later, criminals and foreign governments repeatedly have hacked into government databases and financial institutions. Of course, the SEC must consider these concerns as it finalizes this powerful new repository. While the Consolidated Audit Trail is a powerful regulatory tool, it also represents a high-value target for those seeking to do harm. In order to ensure this vital resource remains a positive for all involved and does not become a threat to market stability or national security, the SEC and the NMS Plan Participants must take robust action to ensure this information is given the protection it requires and that the Consolidated Audit Trail is not susceptible to cyberattack or other forms of information misappropriation. In this vein, we provide a number of comments and recommendations for the Commission to consider for enhancing the CAT NMS Plan.

I. INTRODUCTION

In 2012, the Commission adopted Rule 613 of Regulation NMS under the Securities Exchange Act of 1934, directing NMS Plan Participants to submit a NMS plan to create, implement, and maintain a CAT that would capture customer and order event information for orders in NMS securities, across all markets, from the time of order inception through routing, cancellation, modification, or execution in a single, consolidated data source.[4] Since 2012 however, the nature of personal, commercial, and even national threats has dramatically changed as cybersecurity has moved to the forefront of risks we face as individuals, businesses and as a nation. The list of federal government cyber breaches is long and growing, including the White House (2014), Department of State (2014), Federal Deposit Insurance Corporation (2015, 2016), Federal Aviation Administration (2015), Department of Defense (2015), Internal Revenue Service (2015, 2016), Office of Personnel Management (2015), the Pentagon (2015), and the Federal Reserve (2011-2015).[5] The Commission's own Inspector General recently issued a report suggesting that the SEC should strengthen its protections.[6] Cyber breaches at corporations have

---

[3] Mary Jo White, Chairman's Address at SEC Speaks 2015, Feb. 20, 2015, available at: https://www.sec.gov/news/speech/2015-spch022015mjw.html.

[4] *See* 17 CFR 242.613; *and* Notice *supra* note 2 at p. 7. MFA submitted comments to the SEC's proposed rulemaking on Rule 613 and raised concerns with respect to the confidentiality of customer information and consolidated data.

[5] *See* Continued Federal Cyber Breaches in 2015, Riley Walters, Nov. 19, 2015, available at: http://www.heritage.org/research/reports/2015/11/continued-federal-cyber-breaches-in-2015. *See* The IRS Says Identity Thieves Hacked Its Systems Again, Fortune, Feb. 10, 2016, available at: http://fortune.com/2016/02/10/irs-hack-refunds/; *and* Federal Reserve Hacked More than 50 Times in 4 Years, The Huffington Post, June 1, 2016, available at: http://www.huffingtonpost.com/entry/hackers-breach-federal-reserve-50-times_us_574ee0d5e4b0757eaeb1194c. *See also* Republican Staff Memorandum to Republican Members, Committee on Science, Space and Technology, July 12, 2016 available at: https://www.documentcloud.org/documents/2992789-Final-GOP-Interim-Staff-Report-7-12-16.html.

[6] Office of Inspector General, SEC, Audit of the SEC's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2015, June 2, 2016, Rep. No. 535, available at:

also become a common occurrence, including high profile cyber breaches at Nasdaq, Premera Blue Cross, Anthem, Sony, Home Depot, Ebay and Target.[7] What is more, the nature of warfare and terrorism is also changing as nation-states and cybercriminals target infrastructure.[8] Given this new reality and the large volume of data the Commission already maintains about market participants, we urge the Commission and NMS Plan Participants to carefully weigh the regulatory value of actions taken to implement the CAT against the security risks of exposing such sensitive data. Ideally, the CAT does not expose investors and other market participants to greater risk of a data breach or misappropriation than they face today.

With this important context in mind, MFA believes that it is imperative for the Commission and the NMS Plan Participants to constantly keep data security at the forefront of their considerations with respect to the planning, development and maintenance of the CAT System. We believe the NMS CAT Plan should be designed in a manner that: (1) does not create a new national security vulnerability; (2) mitigates the risk of data security breaches; and (3) allows for the elimination of duplicative filings currently provided by market participants.

II. COMMENTS

A. Governance

The CAT NMS Plan establishes an Operating Committee, consisting of one voting member from each Plan Participant, responsible for managing and implementing the CAT, among other obligations.[9] We believe that the Operating Committee should also include members that represent: an institutional investor, a broker-dealer with a substantial retail base, a broker-dealer with a substantial institutional base, a data management expert and, perhaps more importantly, a representative from a federal agency experienced with cybersecurity concerns as they relate to national security. The decisions of the Operating Committee, such as those relating to data security and funding/fees, will have a significant impact on market participants immediately and in the future. As such, we believe it is important to have market participant representatives on the Operating Committee. In addition, having such representatives will assist with enhancing transparency to the CAT governance process and mitigating potential conflicts of interest.

---

https://www.sec.gov/oig/reportspubs/Audit-of-the-SECs-Compliance-with-the-Federal-Information-Security-Modernization-Act-for-Fiscal-Year-2015.pdf ("**SEC IG Report**")

[7] *See* Michael Riley, How Russian Hackers Stole the Nasdaq, BloombergBusinessWeek, July 21, 2014, available at: http://www.bloomberg.com/news/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq; Keith Collins, A Quick Guide to the Worst Corporate Hack Attacks, Bloomberg, Updated Mar. 18, 2015, available at: http://www.bloomberg.com/graphics/2014-data-breaches/.

[8] *See* NSA Chief Says 'When, Not If' Foreign Country Hacks U.S. Infrastructure, Reuters, Mar. 1, 2016, available at: http://fortune.com/2016/03/01/nsa-chief-hacking-infrastructure/; U.S. Infrastructure Can Be Hacked With Google, Simple Passwords, NBC News, Apr. 3, 2016, available at: http://www.nbcnews.com/news/us-news/u-s-infrastructure-can-be-hacked-google-simple-passwords-n548661; *and* Security Firm Warns of 'Cyber Jihad', CNBC Video, June 16, 2016, available at: http://video.cnbc.com/gallery/?video=3000526401. *See also* Massive US-planned cyberattack against Iran went well beyond Stuxnet, Dan Goodin, arstechnica, Feb. 16, 2016, available at: http://arstechnica.com/tech-policy/2016/02/massive-us-planned-cyberattack-against-iran-went-well-beyond-stuxnet/.

[9] Notice at 14 and Appendix A at 18-19.

Otherwise, we are concerned that market participants will be held captive by an entrenched business model with little ability to influence changes. If the only members of the Operating Committee are NMS Plan Participants, we are concerned that there could be little incentive for such members to make meaningful enhancements to the CAT in the future.

In addition, we recommend that the Commission clarify that the CAT will be subject to the full requirements of Regulation Systems Compliance and Integrity ("Reg SCI"), since the CAT will be a facility of each NMS Plan Participant.[10] The Notice clearly states the Commission's expectation that, at a minimum, the security of the CAT Data must be consistent with Reg SCI.[11] The Notice, however, fails to assure market participants that the CAT will independently comply with the comprehensive policies and procedures and notice provisions required under Reg SCI.[12] Adherence to the oversight and notice provisions of Reg SCI are important to provide the public a minimum level of assurance of the CAT's governance.

Accordingly, MFA recommends that the Commission amend the CAT NMS Plan to require that the Operating Committee for the CAT include voting members that represent: an institutional investor, a broker-dealer with a substantial retail base, a broker-dealer with a substantial institutional base, a data management expert and an expert from a federal agency experienced with cybersecurity concerns as they relate to national security.

B. Data Security and Confidentiality

1. <u>The Security and Confidentiality of Information Reported to the Central Repository</u>

We appreciate that the Notice addresses data security and confidentiality in a number of contexts. We believe the discussion in Appendix C of the CAT NMS Plan, Discussion of Considerations, on the security and confidentiality of information reported to the Central Repository is helpful in providing the public with an understanding of general policies and requirements on the treatment of confidential information.[13]

The CAT NMS Plan contemplates a large number of regulatory staff having access to the CAT System. This broad access greatly increases security risks. Given recent reports by the U.S. Government Accountability Office and SEC Office of Inspector General relating to information

[10] *See* Securities Exchange Act Release No. 73639, 79 Fed. Reg. 72252, 72275 n. 246 (Dec. 5, 2014).

[11] Notice at n. 985.

[12] See Notice, Appendix C-3 ("The Participants also will seek to comply with their obligations related to the CAT under Reg SCI as efficiently as possible. . . . The Participants intend to work together and with the Plan Processor, in consultation with the Commission, to determine a way to effectively and efficiently meet the requirements of Reg SCI without unnecessarily duplicating efforts.")

[13] CAT NMS Plan, Appendix C – 29.

security at the SEC,[14] we believe it would help instill public confidence in the security and confidentiality of information reported to the Central Repository for the Commission, as well as NMS Plan Participants, to provide some transparency with respect to processes and protocols for safeguarding CAT data. We recommend that the Commission and NMS Plan Participants provide greater transparency to the public regarding the protection of non-public, confidential data reported to the Central Repository by the SEC and NMS Plan Participants.

2. Specific Data Security Concerns

In reviewing the CAT NMS Plan and as we described above, we have concerns with the lack of protections for the sensitive data that will be stored in the CAT. While our concerns are broad-reaching, we wanted to focus our comments on the most pressing issues.

Data Security Generally – Request for Comment question 206 asks if commenters "believe that the data security requirements set out in Appendix D are appropriate and reasonable?" We do not believe data security requirements set out in Appendix D, the CAT NMS Plan Processor Requirements, are appropriate or reasonable. Fundamentally, these requirements appear to presume that the greatest harm which might occur were CAT Data compromised is that of identity theft to individuals. Because the CAT will effectively aggregate all market data, it represents a unique opportunity for a nation-state or individual to conduct a broadly and deeply disruptive attack on the market, which would have serious impacts on the global economy. It is estimated that the CAT will aggregate between 30 billion to 120 billion order events per day from more than 2,000 sources.[15] For example, an entity intent on causing harm to the market, or making a profit for itself, that gains access to the trading histories of market participants could reverse engineer their investment strategies and place multiple firms under severe duress simultaneously, triggering massive selling and a catastrophic market event. Because the requirements in the Plan do not contemplate this type of systemic risk, they are insufficient to address the actual risks of the CAT.

We believe that for the CAT NMS Plan data security requirements to be reasonable and appropriate the requirements would need to be drafted with respect to a concretely stated threat model that includes nation-state actors and other well-funded, sophisticated actors who would be willing and able to use the CAT Data to achieve strategic or tactical goals. Accordingly, we recommend that the Commission and/or Plan Participants revise the CAT NMS Plan Processor Requirements to address data security with respect to a threat model that includes nation-state and other well-funded actors.

Data Access – One of the most vital protections that must be in place for the CAT NMS Plan is strict control on access to the CAT data. Appendix D requires that the Plan Processor provide "[p]eriodic reports detailing the current list of authorized users and the date of their most

[14] *See, e.g.*, Information Security: Opportunities Exist for SEC to Improve its Controls over Financial Systems and Data, U.S. Government Accountability Office, April 2016, available at: http://www.gao.gov/assets/680/676876.pdf; *and* SEC IG Report, *supra* note *6*.

[15] *Consolidated audit trail: The CAT's out of the bag*, PwC, June 2016.

recent access . . . to Plan Participants, the SEC and the Operating Committee."[16] We recommend that the Commission amend Section 4.1.4 of Appendix D to require that the Plan Processor provide periodic reports detailing the current list of authorized users, the date of their most recent access, the frequency of access by authorized users, and the categories of data accessed. We believe reporting CAT System access frequency will help establish an understanding for baseline levels of activity, and assist the Plan Processor with detecting abnormal levels of activity. Identifying the category of data access will be fundamental in determining the risk and legal implications of a breach.

Second, we recommend that the Commission amend Section 4.1.4 of Appendix D to require that the Plan Processor maintain access logs for a period of five years. Because the average time that a breach is typically exposed is not until almost a year after its occurrence, we believe it's important for access logs to be maintained for multiple years.

Third, we support the requirement that "[a]ny login to the system that is able to access PII data must follow non-PII password rules and must be further secured via multi-factor authentication."[17] We believe, however, that all persons with access to the CAT System, regardless of ability to access PII data, should have their access secured via multi-factor authentication as prescribed in OMB Memorandum M-06-16, as it has become standard practice; and recommend that the Commission amend the provision accordingly.

Finally, with respect to data access, we strongly oppose the academic access to the CAT suggested in the Notice and Request for Comment question 288. While we appreciate the potential for academic research, given the sensitivity of the data in the CAT, we believe this information should be maintained for regulatory and law enforcement purposes only. It should not be used as a research tool for academics who could use this information in a wide variety of ways that would potentially be counter to the reasons registrants provide this data. It is important to note that detailed records of trade data can reveal the highly sensitive investment strategies of registrants, and as a result CAT Data should not be available to those seeking to use it outside of regulatory and law enforcement capacities.[18]

---

[16] CAT NMS Plan, Appendix D -12.

[17] CAT NMS Plan, Appendix D – 13.

[18] *See, e.g.,* CME Group sparked shutdown of CFTC's academic research program, Reuters, Apr. 24, 2013, (raising concerns that the CFTC illegally shared sensitive market data with researchers who then used the information to publish academic papers about high-frequency trading), available at: http://www.reuters.com/article/cftc-cme-research-idUSL2N0D91IT20130424. *See also,* CFTC OIG Review of the CFTC's Response to Allegations Pertaining to the Office of the Chief Economist, Feb. 21, 2104, available at: http://www.cftc.gov/idc/groups/public/@aboutcftc/documents/file/cftc_046841.pdf. While the CFTC Inspector General did not find indications that the academic articles disclosed information in violation of section 8 of the Commodity Exchange Act, prohibiting disclosure of information that would disclose the business transactions, market positions or trade secrets of any person, market participants remain alarmed that certain academic articles, which have since been removed from web publication, revealed trade secrets of specific market participants.

Updates of Security Plan – Appendix D provides that the CAT System "security plan must be updated annually."[19] We recommend that the Commission amend Section 4.1 of Appendix D to require the Plan Processor to update the security plan as part of an annual review of the security plan; and that the Plan Processor evaluate the security plan against a standard, such as by the National Institute of Standards and Technology or the International Organization for Standardization. While the Notice does not seek comment on this issue, we think providing a clearer standard and process for how security updates will occur is essential.

Connectivity and Data Transfer – Request for Comment question 217 asks "[w]hat are the risks, if any, of allowing Internet access from the Central Repository, even if encrypted?" We believe there are significant risks associated with allowing internet access from the Central Repository. Allowing internet access from the Central Repository greatly increases the risks of a third party unlawfully accessing CAT data. We believe the CAT data is on par with, and meets, the standards for classified information as set in Executive Order 13526 on Classified National Security Information (the "Executive Order").[20] Under the Executive Order, information may be considered for classification if "its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security . . . and it pertains to . . . (e) scientific, technological, or economic matters relating to the national security"[21] We think that unauthorized disclosure or use of CAT data could destabilize the U.S. and world financial markets by causing investor panic, mass selling and runs on financial institutions. The potential extent of damage to the U.S. markets and economy would be a matter of national security.

As the CAT data meets the standards for classification, we believe that it should be handled in a comparable manner as classified information and that the SEC, NMS Plan Participants, the Plan Processor and any others with access to CAT data should use a higher degree of care in handling such data. The SEC, NMS Plan Participants and the Plan Processor should consider the standard government protocols for handling sensitive data in the national security framework. In response to Request for Comment question 223, we believe Federal Information Processing Standard ("FIPS") 199 data categorization standards should apply. The frameworks used by government, both for classification and protection, should guide the limits on connectivity and transfer of CAT data.

Additionally, Appendix D provides that "CAT Reporters must connect to the CAT infrastructure using secure methods such as private lines or . . . Virtual Private Network connections over public lines."[22] Given the security implications surrounding this data, we do not believe remote access as suggested in 4.1.1 of Appendix D is appropriate. In relying on the FIPS standards, such access is not appropriate for material of this importance.

---

[19] CAT NMS Plan, Appendix D – 10.

[20] *See* Executive Order 13526 – Classified National Security Information, Dec. 29, 2009, available at: https://www.gpo.gov/fdsys/pkg/DCPD-200901022/pdf/DCPD-200901022.pdf.

[21] *Id. at Sec. 1.4.*

[22] CAT NMS Plan, Appendix D – 11.

Data Encryption – Strong encryption should be at the heart of the CAT NMS Plan's efforts to protect data. Request for Comment question 216 asks if we "believe that the Plan's data encryption requirements are adequate for CAT Data and PII Data [and if the Plan] provides sufficient information and clarity regarding data encryption requirements." We believe that the CAT NMS Plan's encryption requirements alone are not sufficient to protect CAT data and PII data. There are many more detailed and technical issues that must be considered in order for the encryption requirements for the CAT System and data to be sufficient. Accordingly, we recommend that the SEC and NMS Plan Participants ensure that those implementing the CAT have extensive experience in securing sensitive data. In addition, we recommend that the CAT NMS Plan require that data is encrypted both in flight, as well as at rest; and that particularly sensitive pieces of data are isolated or compartmentalized. In this way, a data breach in one area of the CAT System does not jeopardize the security of all data.

To the extent that CAT data needs to be archived, apart from disaster recovery and business continuity plan requirements, we recommend that the Commission amend Section 4.1.2 of Appendix D to clarify that the monitoring, alerting, auditing, and any other requirements that apply with respect to CAT data also applies to archival CAT data. With respect to data storage, we oppose the use of public cloud storage, as discussed further below; however, if cloud storage is used, the encryption keys should not be stored in maintained in cloud storage.

Data Storage and Environment – Request for Comment question 42 asks whether the CAT NMS Plan should mandate a particular data storage method. We believe the CAT NMS Plan should not mandate a particular data storage method, because the CAT NMS Plan should provide enough flexibility for the Plan Processor to use the best technology at any time. Mandating a particular data storage method is likely to tie the Plan Processor to the best data storage technology of 2016. Nevertheless, as a current matter, we have strong concerns with the use of public cloud storage. We are concerned of the security of such storage facility; that by using a public cloud storage system, the Plan Processor would lose control over the data; and that there is not likely to be meaningful recourse against a cloud data storage provider in the event of a breach.

Section 4.1.3 on Data Storage and Environment in Appendix D requires that the "Plan Processor must include penetration testing . . .".[23] We believe the requirements should go further and recommend that the Commission amend Section 4.1.3 of Appendix D to require that the Plan Processor conduct internal vulnerability assessments as part of the requirement to perform penetration testing. The Plan Processor should also consider the use of a bug bounty program, which awards individuals who report software bugs, especially those pertaining to exploits and vulnerabilities, with recognition and compensation. Bug bounty programs have become an effective way for companies to discover and resolve bugs more quickly; and are widely used by companies, including Google, facebook, and Yahoo, among others.[24]

---

[23] CAT NMS Plan, Appendix D – 12.

[24] *See, e.g.*, information on Google's bug bounty program available at: https://www.google.com/about/appsecurity/reward-program/; information on facebook's bug bounty program available at: https://www.facebook.com/whitehat; *and* information on Yahoo's bug bounty program available at: https://yahoo.github.io/secure-handlebars/bugBounty.html.

4.1.5 Breach Management – Appendix D requires that the Plan Processor develop a cyber incident response plan.[25] We recommend that the Commission amend section 4.1.5 of Appendix D to define a "reportable incident" that would trigger implementation of the cyber incident response plan, notwithstanding local state law requirements with respect to information security breaches. We also recommend that the Commission amend section 4.1.5 of Appendix D to require the Plan Processor to abide by local state laws regarding security breach notifications; and to promptly notify a customer when his or her trading data has been compromised regardless of whether PII data was included or compromised. A security breach of a customer's trading data could compromise the customer's investment strategies even if the customer's PII was not compromised. As such, we believe it is important for the Plan Processor to notify a customer of security breaches in order for the customer to begin taking steps to mitigate the breach.

C. Reducing Form Filings

The CAT NMS Plan will provide regulators with detailed and comprehensive trading and position information of market participants, and afford regulators the ability to conduct and produce regular market reports. We believe the Commission in approving a CAT NMS Plan should take the opportunity to eliminate filing requirements that will become unnecessary as a result of the information available to regulators from the CAT System, such as Rule 13h-1 and Form 13H regarding Large Trader filings.[26] The Commission adopted the large trader reporting requirements to receive data to help it better understand the market activities of large traders and their role in the securities markets. In particular, the Commission was interested in execution order time and the ability to identify participants that effected large trades.[27] With the CAT data, SEC staff will have access to the same information that they are receiving through Form 13H. Repealing Rule 13h-1 and the Form 13H filing requirement would eliminate the need by market participants to file duplicative information; and would reduce regulatory costs and burdens on market participants, who would otherwise have to bear the costs of filing large trader reports and fees associated with the development and maintenance of the CAT. Accordingly, we recommend that the Commission repeal Rule 13h-1 and Form 13H once it begins receiving complete CAT data.

* * * * *

[25] *Id.*

[26] *See* 17 CFR 240.13h-1; *and* Large Trader Reporting Final Rule, SEC Release No. 34-64976, available at: https://www.sec.gov/rules/final/2011/34-64976.pdf.

[27] *See id.*

MFA appreciates the opportunity to provide comments and recommendations on the CAT NMS Plan. We would welcome the opportunity to discuss our comments with the Commission or its staff in greater detail. If the staff has any questions, please do not hesitate to contact Jennifer Han, Associate General Counsel, or the undersigned at (202) 730-2600.

Respectfully submitted,

/s/ Stuart J. Kaswell

Stuart J. Kaswell
Executive Vice President & Managing Director,
General Counsel
Managed Funds Association