Managed Funds Association
The Voice of the Global Alternative Investment Industry
Washington, D.C. | New York

December 2, 2020

Via Electronic Submission: rule-comments@sec.gov

Ms. Vanessa Countryman
Secretary
Securities and Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549-1090

Re: Proposed Amendments to the National Market System Plan Governing the Consolidated Audit Trail to Enhance Data Security (File No. S7-10-20)

Dear Ms. Countryman:

Managed Funds Association[1] (**"MFA"**) appreciates the opportunity to comment on the Securities and Exchange Commission's proposed amendments to the national market system plan governing the consolidated audit trail ("**CAT NMS Plan**" or "**Plan**").[2] The proposed amendments are designed to enhance the security of the Consolidated Audit Trail ("**CAT**") and to limit the scope of sensitive information required to be collected by the CAT.

Data security and cybersecurity are some of the top concerns for MFA and its members. As we stated in our prior comment letters on the CAT,[3] while the CAT is a powerful regulatory tool, it also represents a high-value target for those seeking to do harm. Therefore, in order to ensure that the CAT does not become a threat to market stability or national security, it is imperative for the Commission and CAT Participants to constantly keep data security at the forefront of their considerations with respect to the planning, development and maintenance of the CAT. This will help ensure that the CAT is not susceptible to cyberattack or other forms of information misappropriation, and that the risk of data security breaches is mitigated.

[1] MFA represents the global alternative investment industry and its investors by advocating for public policies that foster efficient, transparent, fair capital markets, and competitive tax and regulatory structures. MFA supports member business strategy and growth via proprietary access to subject matter experts, peer-to-peer networking, and best practices. MFA's more than 140 member firms collectively manage nearly $1.6 trillion across a diverse group of investment strategies. Member firms help pension plans, university endowments, charitable foundations, and other institutional investors to diversify their investments, manage risk, and generate attractive returns over time. MFA has a global presence and is active in Washington, London, Brussels, and Asia, supporting a global policy environment that fosters growth in the alternative investment industry.

[2] Securities Exchange Act Release No. 34-89632, 85 FR 65990 (August 21, 2020).

[3] *See, e.g.*, letter from Stuart J. Kaswell, Executive Vice President & Managing Director, General Counsel, MFA, to Brent J. Fields, Secretary, SEC, on June 23, 2017 on Proposed Rule Changes to Establish Fees for Industry Members to Fund the Consolidated Audit Trail, available at https://www.managedfunds.org/wp-content/uploads/2020/04/MFA-Ltr-SEC-Review-of-CAT-Fees.final_.7.28.17.pdf, and letter from Stuart J. Kaswell, Executive Vice President & Managing Director, General Counsel, MFA, to Brent J. Fields, Secretary, SEC, on July 18, 2016 on the Consolidated Audit Trail, available at https://www.managedfunds.org/wp-content/uploads/2020/04/MFA-Letter-on-SEC-Consolidated-Audit-Trail.pdf.

In this vein, we appreciate the Commission's continued attention to these matters and we strongly support the proposed amendments. We believe the amendments go far in addressing prior MFA concerns surrounding the security of the Plan, as well as associated MFA recommendations around the need for better safeguards and protection of information contained in the CAT, mitigating the risk of data security breaches, providing greater transparency to the public regarding the protection of non-public, confidential data reported to the CAT, and stricter controls on access to CAT data and recordkeeping around such access.

While we support the proposal, we have several comments and recommendations to further enhance the efficiency of the Plan. Our specific comments follow.

I. Secure Analytical Workspaces

The proposal would require the creation and use of Secure Analytic Workspaces ("**SAWs**")[4] where CAT Data[5] would be accessed and analyzed by Plan Participants. The Plan Processor would be required to provide a SAW account for each Participant that implements all of the common technical security controls required by the Plan's Comprehensive Information Security Program. The Commission states the use of SAWs would facilitate efforts to: minimize the "attack surface" associated with CAT Data; maximize security-driven monitoring of CAT Data; and leverage security controls and related policies and procedures that are consistent with those that protect the Central Repository.

MFA supports requiring the use of SAWs, and particularly requiring that "Customer and Account Attributes Data," i.e., personally identifiable information, can only be viewed in the SAW given the sensitive nature of such data.[6] We agree with the Commission that it is of utmost importance that access to, and extraction of, Customer and Account Attributes data is provided the most stringent level of protection, which can only be provided through the use of a SAW environment.

We note that the proposal sets forth a process by which Participants may be granted an exception from the requirement to use a SAW to access CAT Data, for example, to reduce burdensome costs and/or operational complexity. Specifically, Participants seeking an exception to the SAW usage requirements would be required to provide the Chief Information Security Officer of the Plan Processor (the "**CISO**"), the Chief Compliance Officer, the members of the Security Working Group and their designees (discussed below), and Commission observers of the Security Working Group with certain information regarding the non-SAW environment. Such information would include a security assessment of the non-SAW environment and detailed design specifications for the environment demonstrating the extent to which the non-SAW environment's design specifications adhere to the design specifications developed by the Plan Processor for SAWs.

---

[4] A "Secure Analytical Workspace" is defined as "an analytic environment account that is part of the CAT System, and subject to the Comprehensive Information Security Program, where CAT Data is accessed and analyzed by Participants pursuant to Section 6.13."

[5] "CAT Data" is defined as "data derived from Participant Data, Industry Member Data, SIP Data, and such other data as the Operating Committee may designate as 'CAT Data' from time to time."

[6] MFA strongly supports no longer requiring Industry Members to report certain personally identifiable information such as social security numbers/individual taxpayer identification numbers and account numbers in accordance with the exemptive order issued by the Commission on March 17, 2020.

While we acknowledge the need to have exceptions under certain circumstances, any exceptions in this area should be granted on an extremely limited basis and be used solely for regulatory purposes. In addition, the standards and processes around granting any exceptions should be robust and as stringent as possible.[7] To that end, we would support requiring a Participant seeking an exception to provide additional information such as a detailed description of the regulatory or surveillance activities that they plan to conduct with the CAT Data accessed from the non-SAW environment. In addition, we would support requiring the Commission to either formally approve, or not-object to, the granting of such an exception.

II. Security Working Group

To provide support and additional resources to the CISO and the Operating Committee of the CAT NMS Plan, the proposed amendments would require the permanent establishment of a security working group ("**Security Working Group**") that will be composed of the CISO and the chief information security officer or deputy chief information security officer of each SRO that is a participant to the Plan. The CISO and the Operating Committee would be allowed to invite other parties to attend specific meetings to enable the Security Working Group to obtain a broad range of views and to present such views to the CISO and the Operating Committee on key security issues.

MFA previously raised concerns regarding the governance of the CAT NMS Plan. Specifically, we recommended that the Operating Committee should include market participant representatives, including an institutional investor, as the decisions of the Operating Committee will have a significant impact on market participants immediately and in the future. We believed, and continue to believe, that having market participant representatives directly involved in the CAT governance process would assist with enhancing transparency to the process and mitigating potential conflicts of interest. Market participants deserve to have a voice in a system that affects them, and have the ability to provide constructive feedback and influence changes to the CAT.

While the CAT NMS Plan currently has an Advisory Committee to advise the SROs on the implementation, operation, and administration of the CAT that includes institutional investor representation, we believe such a requirement should be extended to the Security Working Group. Inclusion of industry representatives on the Security Working Group can assist in addressing conflicts of interest and can serve as a valuable resource in assisting in the protection of customer data.

We therefore recommend that the Security Working Group be expanded to include CISOs, or persons with similar roles, from other market participants, including institutional investors. Given the sensitive nature of the issues that would be discussed at meetings of the Security Working Group, we would support requiring non-SRO representatives to sign a non-disclosure agreement or to adhere to some other protocol designed to prevent the release of confidential information regarding the security of the CAT System, such as being subject to the appropriate confidentiality obligations set forth in the CAT NMS Plan.

[7] The proposal provides that the Chief Information Security Officer and the Chief Compliance Officer may jointly grant an exception if they determine, in accordance with policies and procedures developed by the Plan Processor, that the residual risks identified in the security assessment or detailed design specifications provided pursuant to Section 6.13(d)(i)(A) do not exceed the risk tolerance levels set forth in the risk management strategy developed by the Plan Processor for the CAT System pursuant to NIST SP 800-53.

III. Participants' Confidentiality Policies and Procedures

The proposed amendments would require the Participants to establish, maintain and enforce identical written data confidentiality policies. Each Participant also would establish, maintain and enforce procedures and usage restrictions in accordance with these policies. Among other things, the policies must: (1) be reasonably designed to ensure the confidentiality of CAT data obtained from the Central Repository and limit the use of the data solely for surveillance and regulatory purposes; (2) limit extraction of CAT Data to the minimum amount necessary to achieve a specific surveillance or regulatory purpose; (3) limit access to CAT Data to persons designated by Participants, who must be "Regulatory Staff," or technology and operations staff that require access solely to facilitate access to and usage of the data by Regulatory Staff; (4) implement effective information barriers between the Participants' Regulatory Staff and non-Regulatory Staff with regard to access and use of CAT Data; (5) only allow access to CAT data where there is a specific regulatory need for such access; and (6) document monitoring and testing protocols that will be used to assess Participant compliance with the policies. Significantly, the proposal notes that Participant staff who primarily perform commercial or business functions generally should not have access to CAT Data.

MFA strongly supports these requirements. We believe that such restrictions and controls should help limit access to CAT Data, both to the individuals with access to CAT Data and the amount of CAT Data used by these individuals. In addition, limiting the access of an individual to only the specific data required for that individual's surveillance or regulatory function would reduce the potential of inappropriate receipt and misuse of sensitive CAT Data.

The proposal would require the Participants to make the policies publicly available on each of the Participants' websites, or collectively on the CAT NMS Plan website. The proposal states that the Commission believes that public disclosure of the policies could help encourage the Participants to create robust policies because they will be subject to public scrutiny. The Commission also believes that such a requirement would allow other Participants, broker-dealers, investors, and the public to better understand and analyze the policies that govern Participant usage of, and the confidentiality of, CAT Data.

We agree with the Commission's assessment. However, while we support the proposed transparency around confidentiality policies, we believe the Commission should go one step further and subject the policies to a public notice and comment period to allow market participants to have real input into the policies, which will be an important tool to safeguard CAT data. In particular, the Commission could subject the policies to a public comment process either through the SRO rule filing process under Section 19(b)(1) of the Exchange Act or as an amendment to the CAT NMS Plan.

IV. Limiting Access to CAT Data to Non-Commercial Purposes

The Commission proposes to specify that Regulatory Staff and the Commission must be performing regulatory functions when using CAT Data, including for economic analyses, market structure analyses, market surveillance, investigations, and examinations, and may not use CAT Data in such cases where use of the data may serve both a surveillance or regulatory purpose, and a commercial purpose. The Commission further proposes that in any case where the use of CAT Data may serve both a surveillance or regulatory purpose and a commercial purpose, such as economic analyses or market structure analyses in support of SRO rule filings with both a regulatory and commercial purpose, use of CAT Data is not permitted.

MFA supports these restrictions. We believe that addressing conflicts of interest in the securities markets is significant to ensure fair and orderly markets for MFA members and other market participants. This is especially important given the for-profit models of the exchanges and the continued pressures on exchanges to find ways to generate revenue, sometimes contrary to the interests of investors. To that end, we support calls to restrict an exchange's access to CAT Data to data for trading activity conducted on that particular exchange, with limited exceptions for situations in which an exchange has well-defined and articulated regulatory purposes to look at the trading data of another exchange under their rules or the rules of the Commission.

V. Application of the Proposed Amendments to Commission Staff

The CAT NMS Plan contemplates a large number of persons having access to the CAT system, including Commission personnel. While the proposed amendments restrict access to CAT data, security risks remain.

The proposal states that the Commission takes very seriously concerns about maintaining the security and confidentiality of CAT data and believes that it is imperative that the Commission implement and maintain a robust security framework with appropriate safeguards to ensure that CAT data is kept confidential and used only for surveillance and regulatory purposes. The proposal notes, however, that the Commission is not a party to the CAT NMS Plan and that the Commission does not believe that it is appropriate for its security and confidentiality obligations, or those of its personnel, to be reflected through CAT NMS Plan provisions.

While we appreciate the reasons for the need for different mechanisms from Participants for Commission personnel with respect to the security and confidentiality of CAT data, we believe it will be critical for Commission personnel to be subject to stringent and robust data security and confidentiality standards, at the very least in line with those applicable to Plan Participants and their personnel.

* * * * *

We appreciate the opportunity to provide these comments on the proposed amendments. If you have any questions about these comments, or if we can provide further information, please do not hesitate to contact me at (202) 730-2600.

Respectfully Submitted,

/s/ Jennifer W. Han

Jennifer W. Han
Managing Director & Counsel, Regulatory Affairs

cc: The Honorable Jay Clayton, Chairman
The Honorable Hester M. Peirce, Commissioner
The Honorable Elad L. Roisman, Commissioner
The Honorable Allison Herren Lee, Commissioner
The Honorable Caroline A. Crenshaw, Commissioner