VIRTU FINANCIAL

January 27, 2021

VIA ELECTRONIC DELIVERY

Ms. Vanessa A. Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

RE: Joint Industry Plan; Notice of Filing of Amendment to the National Market System Plan Governing the Consolidated Audit Trail by the Plan Participants (Release No. 34-90826; File No. 4-698)

Dear Ms. Countryman:

Virtu Financial, Inc. (together with its affiliates, "Virtu" or "we")[1] respectfully submits this letter in response to the above-referenced notice of proposed amendments (the "Proposal") to the National Market System Plan Governing the Consolidated Audit Trail (the "CAT NMS Plan") submitted by the Operating Committee for Consolidated Audit Trail, LLC ("CAT LLC") on behalf of the parties to the CAT NMS Plan (collectively, the "Plan Participants"). Among other items, the Proposal would effectively absolve the CAT LLC and the Plan Participants of virtually all liability for harm caused by a data security breach or misuse of data reported to the CAT ("CAT Data") and shift that liability to the members of the financial services industry ("Industry Members") who are required by law to report the CAT Data but have absolutely no control over the CAT Data after it is reported to CAT LLC.

Virtu strongly objects to the Proposal on the basis that it is unfair, inefficient, anti-competitive, and just plain illogical. Under the rule set governing the CAT, Industry Members are obligated by law to report a wide array of sensitive transaction data related to the lifecycle of an order including, but not limited to, quotes, original receipts or originations of an order, modifications, cancellations, routing, receipts of a routed order execution, and order allocations. Once the CAT Data is reported to CAT LLC, Industry Members have absolutely no role in managing, controlling, or protecting it from breach or misuse. Control and management of the CAT Data rests solely with the Plan Participants, and CAT LLC is wholly responsible for securing the data and protecting it from being compromised.

---

[1] Virtu is a leading financial firm that leverages cutting edge technology to deliver liquidity to the global markets and innovative, transparent trading solutions to its clients. Virtu operates as a market maker across numerous exchanges in the U.S. and is a member of all U.S. registered stock exchanges. Virtu's market structure expertise, broad diversification, and execution technology enables it to provide competitive bids and offers in over 25,000 securities, at over 235 venues, in 36 countries worldwide. As such, Virtu broadly supports innovation and enhancements to transparency and fairness which enhance liquidity to the benefit of all marketplace participants.

Shifting liability to the Industry Members for potential harm caused by the compromise of CAT Data over which they have no control and which they are not responsible for securing is a heavy handed approach that is completely misaligned with the structural and economic realities of how the CAT was designed to operate. For the reasons described below, we encourage the Commission to follow the equities and disapprove CAT LLC's ill-conceived Proposal.

The Controller of Data Should be Liable

First and foremost, the Proposal is directly at odds with the basic and obvious principle that the entity that has control of the CAT System and CAT Data – and that is obligated by law to take on the responsibility of securing it – should assume liability for any failure in implementing security that leads to a breach. There can be no other logical outcome, especially where, as here, the Industry Members have absolute control of the CAT Data and no ability to control how CAT LLC or the Plan Processor secure the data and protect against cyber intrusions.

Under the CAT regulations, CAT LLC's Operating Committee, and the Plan Processor it selects and controls, are responsible for holding the reported data and for keeping it secure. Indeed, CAT LLC highlights its responsibilities specifically in the Frequently Asked Questions ("FAQs") for the CAT:

> "**FAQ S.1. What steps are being taken to ensure that the CAT is secure given heightened cybersecurity concerns?**
> The CAT NMS Plan requires the Plan Processor, subject to the oversight of the Operating Committee, to develop a comprehensive information security program that addresses the security and confidentiality of all information accessible from the CAT and the operational risks associated with accessing the CAT. Appendix D of the CAT NMS Plan sets forth minimum data security requirements for the CAT that the Plan Processor must meet. In addition, as required by the Plan, the Plan Processor has designated a Chief Information Security Officer (CISO), who is responsible for, among other things, creating and enforcing appropriate policies, procedures, and control structures regarding data security."[2]

By design, once they have reported CAT Data as required by law, the Industry Members have no control over the data or its security. They have no input into the security and risk mitigation measures that CAT LLC and the Plan Processor should implement, no oversight or control of the CAT database itself, and no ability to control who accesses or downloads information from the CAT. When it is fully rolled out, the CAT system will be one of the largest repositories of customer and trading financial information in the world. It will be a possible target for data breaches and cybercrime. This risk is amplified because employees of the Plan Participants will be permitted to download data onto their servers, creating yet more targets for cyber intrusion.

[2] CAT NMS Plan Frequently Asked Questions, available at https://www.catnmsplan.com/faq.

It is illogical and unfair to require Industry Members to take on liability for this risk when they have no ability to control the data or protect against a breach.[3] The Plan Participants are exclusively responsible for maintaining the CAT System and for implementing measures to protect against a breach, and therefore liability should rest with them.

What's more, shifting liability to the Industry Members would also result in a dramatic misalignment of incentives. Surely, the Commission has in interest in fostering incentives to make the CAT Data as secure as possible. If the Plan Participants are liable, they will have an incentive to invest in security measures. If they are not liable, they will have no incentive to have a best-in-class security framework. Shifting liability to Industry Members will not incentivize security because they have no control over the CAT's security – even if the Industry Members wanted to enhance security, it is the Plan Participants who make the final decisions. Keeping liability with the Plan Participants is essential to incentivizing them to protect the CAT Data.

Industry Member Liability Construct May Be Uninsurable

As the Plan Participants readily acknowledge, CAT LLC and the Plan Processor have access to cyber insurance, and they are clearly in a far better position to insure against risks to data under their control, at a much lower cost, than are individual Industry Members. But even more important as a threshold issue, we are skeptical that Industry Members could obtain insurance policies under the current CAT System construct. In our experience, cyber insurance policies have significant limitations and are not a panacea in the event of a breach. Here, other than in connection with an Industry Member's direct transmission of data to the CAT, a firm's cyber insurance policy may not cover risk of loss, especially given that the Industry Members have no control over the data it is by law required to submit, its security or the CAT systems.

Indeed, if anything, Industry Members should be added as "additional insured parties" under CAT LLC's own cyber insurance policies given the significant risk that is associated with the requirement that they report highly sensitive customer and transaction data to the CAT. Without any ability to control the data after it is reported to CAT LLC, the Industry Members are exposed to a high degree of litigation risk in the event of breach or misuse that they should not be forced to self-insure, and therefore should be covered by the insurance policies of the Plan Participants.

Even if, hypothetically, the Industry Members could obtain the requisite insurance, it would be dramatically inefficient, unfair, and illogical to adopt an alternative liability construct in which hundreds of firms – which are being forced by regulation to submit data to the CAT – incur very significant costs to enhance their individual insurance coverages to address the same and

[3] As the Commission is aware, CAT LLC's Operating Committee approved a draft "Reporter Agreement" in August 2019 with limitation of liability provisions substantially similar to those contained in the Proposal. Despite our strong objection to those provisions, CAT LLC refused to remove the liability provisions. As a consequence, Virtu (and over 1,300 other industry members) signed the Reporter Agreement because we felt we had no other choice in order to test our ability to access the CAT. Our execution of that agreement should not be construed as an acceptance of limited liability by the Plan Participants. To the contrary, it demonstrates the heavy handed approach the Plan Participants have taken throughout the rollout of the CAT and is yet another example of an effort to force the industry to assume responsibilities that appropriately belong to CAT LLC.

overlapping core risks of data breach or misuse within the CAT System. If the Plan Participants retain liability, they will be appropriately incentivized to invest in insurance and other risk mitigation measures. Moreover, under the CAT regulations, Industry Members will be responsible for sharing equitably in the financial burden of the Plan Participants' insurance costs and risk mitigation, without needless overlapping efforts and expenditures. This is far and away a more responsible and economically efficient approach to liability, and one that will ultimately benefit the investing public by eliminating needless and superfluous costs borne by the industry writ large.

Plan Participants' Arguments Are Unpersuasive and Unsupported

The arguments proffered by the Plan Participants in support of shifting liability to the Industry Members are, as the saying goes, "thin soup".

For example, their contention that liability for the CAT should be modeled after the construct used for OATS reporting is a red herring. While it is true that the Plan Participants do not have liability for data breaches under OATS, there can be no dispute that the CAT is a very different animal with exponentially greater risks of cyber intrusion and misuse of sensitive transaction data. First, OATS does not contain highly sensitive information about the identity and transaction history of individual customers. Even with the exclusion of Personally Identifiable Information ("PII"), which Virtu strongly supports, the CAT still contains a wide array of customer-specific information that is not reported through OATS. Second, OATS captures only a fraction of the data that the CAT will contain – no exchange data, market maker orders, customer identifying information, or any information regarding options orders or executions. Third, OATS does not have account-level data that presents the risk of reverse engineering trading strategies using OATS data. And fourth, OATS data is only reported to and used by FINRA, whereas CAT Data is reported to twenty-four Plan Participants and accessible by dozens more employees. OATS should not be a proxy, and risk of loss is so great with CAT that it should be viewed on its own and liability should attach to the Plan Participants.

Furthermore, the positions the Plan Participants have been advocating on CAT security don't seem to square up. On the one hand the Plan Participants have articulated their opposition to the CAT Data Security Proposal,[4] arguing that additional security measures are not needed. For example, in a comment letter opining on the CAT Data Security Proposal, the Plan Participants explicitly state and acknowledge the "robust" nature of the CAT's security profile:

> "**The Current Security Profile of the CAT is Robust**: The Participants believe, and as noted in the Proposing Release, the Commission has concurred that a robust security system has been developed and implemented for the CAT. The Participants, in concert with the Plan Processor, regularly assess the security of the CAT, and actively consider whether and how the security of the CAT can be enhanced on an ongoing basis. Without a clear understanding of how the proposals will materially enhance the current security profile of the CAT, it is difficult to assess them from a cost benefit perspective or in light of the impact they would have on the Participants' ability to complete the scheduled development and

[4] *See* Release No. 34-89632 (August 21, 2020), 85 FR 65990 (October 16, 2020).

> implementation of the CAT or to perform their self-regulatory functions. Given the acknowledged stringent security of the CAT, as well as these and other concerns discussed below, the Participants recommend that the SEC not move forward with the proposal."[5]

At the same time, however, in the present Proposal on liability, the Plan Participants assert that they should not be held liable because the risk of a security breach is too great. Conveniently, when it suits their objectives, the Plan Participants are quick to take credit for the "robust" nature of the security protections they have designed. But when it comes down to who holds the bag in the event of a breach or other misuse or the CAT Data, they are not prepared to stand behind the integrity of the CAT System's security protocols and instead would foist responsibility to Industry Members who have no role in protecting the data.

Finally, the purported economic analysis submitted by the Plan Participants is woefully inadequate and flawed and should not be relied upon. First, its analysis of the likelihood of a cyber intrusion focuses only external actors. It fails to assess the potential of a breach caused by or implemented by Plan Participant personnel. This is a very significant gap, given that potentially dozens of Plan Participant personnel will have access to the CAT system's sensitive data, and many will have license to download that data directly to the Plan Participants' servers. Second, the analysis concludes that ex ante regulatory approach is better than ex post litigation approach because the costs of litigation to the Plan Participants is high and benefits are low, thus no economic justification for allowing additional litigation. However, the analysis fails to take account of the costs to individual Industry Members associated with a cyber-breach of the CAT involving data provided by those firms. This one sided analysis fails to address cost/benefit as it relates to industry participants and therefore should not be relied upon.

In sum, we find their arguments unpersuasive and unsupported, and urge the Commission to digest them with a heavy dose of skepticism.

---

[5] Letter from Michael Simon, Chair of CAT NMS Plan Operating Committee, to Vanessa Countryman (Dec. 4, 2020), available at https://www.sec.gov/comments/s7-10-20/s71020-8100247-226195.pdf

Virtu appreciates the opportunity to submit this response to the Plan Participants' proposed amendments to the CAT NMS Plan. While we acknowledge the underlying goals and objectives of the CAT, we are very concerned about the very significant impact to the marketplace if the Plan Participants are shielded from liability for their actions related to controlling and protecting CAT Data. As a large market making firm, Virtu is required by law to report vast quantities of sensitive transaction data to the CAT, but has no role in protecting it after transmission to the Plan Participants. Aside from being illogical and unfair, shifting liability to Industry Members like us will result in extraordinary and needless costs that will ultimately be borne by everyday retail investors. It would also misalign incentives and amount to a burden on competition. For these reasons, we urge the Commission to reject the Proposal.

Respectfully submitted,

Thomas M. Merritt
Deputy General Counsel

cc: Allison H. Lee, Acting Chairman
Hester M. Peirce, Commissioner
Elad L. Roisman, Commissioner
Caroline A. Crenshaw, Commissioner
Christian Sabella, Acting Director, Division of Trading and Markets