sifma

Invested in America

May 3, 2021

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

Re: ***File No. 4-698; Joint Industry Plan; Order Instituting Proceedings to Determine Whether to Approve or Disapprove an Amendment to the National Market System Plan Governing the Consolidated Audit Trail—Comment Letter of the Securities Industry and Financial Markets Association***

Dear Ms. Countryman:

On behalf of its member firms and the customers they represent, the Securities Industry and Financial Markets Association ("SIFMA")[1] respectfully submits this letter to the U.S. Securities and Exchange Commission (the "Commission") to comment on the above-referenced order (the "Order") by the Commission.[2] The Order extends the time for Commission action on the proposed amendment (the "Proposal")[3] to the National Market System Plan Governing the Consolidated Audit Trail (the "CAT NMS Plan") that is proposing to force all industry members ("Industry Members") that are obligated to report to the Consolidated Audit Trail (the "CAT") pursuant to Commission and self-regulatory organization ("SRO") rules effectively to assume all of the liability associated with a breach or misuse of data in the CAT System, which has been developed and is operated exclusively by the SROs.[4] The Proposal would accomplish this by amending the CAT NMS Plan to require Industry Members and their reporting agents each to

---

1 SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our members, we advocate for legislation, regulation and business policy, affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit http://www.sifma.org.

2 See Release No. 34-391487 (April 6, 2021), 86 FR 19054 (April 12, 2021).

3 See Release No. 34-90826 (December 30, 2020), 86 FR 591 (January 6, 2021).

4 Capitalized terms used in this letter have the same meanings as they do in the CAT NMS Plan. For instance, "CAT Data" and "CAT System" are defined in Article I, Section 1.1 of the CAT NMS Plan. 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." CAT System is defined as "all data processing equipment, communications facilities, and other facilities, including equipment, utilized by the [CAT LLC] or any third parties acting on [CAT LLC's] behalf in connection with operation of the CAT and any related information or relevant systems pursuant to [the CAT LLC Agreement]."

sign a mandatory agreement as a condition of reporting to the CAT that effectively eliminates the liability of CAT LLC and the SROs as the participants of the CAT NMS Plan ("Participants") in the event of a breach or misuse of CAT Data.[5] As we noted in our January 27, 2021 comment letter on the Proposal ("January Comment Letter"), SIFMA continues to object strongly to the Proposal and believes that the Commission should disapprove it in its current form.[6] Our comments below respond to the Commission's Order to determine whether to disapprove the Proposal or to approve the Proposal with any changes or subject to any conditions the Commission deems necessary or appropriate after considering public comment.

I. Background

The Participants submitted the Proposal along with a supporting economic analysis prepared by Charles River Associates (the "CRA Paper") to the Commission on December 18, 2020. The Proposal would revise the CAT Reporter Agreement (the "Reporter Agreement") and the CAT Reporting Agent Agreement (the "Reporting Agent Agreement") to insert limitation of liability provisions (the "Limitation of Liability Provisions") that would strictly limit the SROs' liability in the event of a breach of the CAT System or a misuse of CAT Data by the SROs or their employees. As proposed, the Limitation of Liability Provisions would: (1) provide that CAT Reporters and CAT Reporting Agents accept sole responsibility for their access to and use of the CAT System, and that CAT LLC makes no representations or warranties regarding the CAT System or any other matter; (2) limit the liability of CAT LLC, the Participants, and their respective representatives to any individual CAT Reporter or CAT Reporting Agent to the lesser of the fees actually paid to CAT for the calendar year or $500; (3) exclude all direct and indirect damages; and (4) provide that CAT LLC, the Participants, and their respective representatives shall not be liable for the loss or corruption of any data submitted by a CAT Reporter or CAT Reporting Agent to the CAT System.

In our January Comment Letter, we demonstrated that the Proposal is unsupportable as a matter of public policy, is inconsistent with economic principles as applied to the actual facts and should not be approved by the Commission. In particular, we noted that permitting the SROs to disclaim liability for a breach or misuse of CAT Data (and to shift those risks entirely to individual Industry Members) is fundamentally unfair because the SROs are exclusively responsible for maintaining the CAT System and for implementing measures to protect against a breach of the CAT System. In addition to exposing Industry Members to enormous and unfair liability risks, we noted that the Proposal would allow CAT LLC to under-invest in data security and cyber insurance, and that this approach is inefficient as a matter of risk mitigation and

---

[5] The limitation of liability embodied in the Proposal would extend to nearly every person or entity involved in operating or maintaining the CAT System, as by its terms it applies to CAT LLC, each of the Participants, "the Plan Processor and any other subcontractors of the Plan Processor or CAT LLC providing software or services within the CAT System, and any of their respective affiliates and all of their directors, managers, officers, employees, contractors, subcontractors, advisors and agents." Proposal, Appendix E at paragraph 5.5. Under the Proposal, the maximum liability for each of these entities or individuals pursuant to any CAT Reporting Agreement in any calendar year would be $500. Id.

[6] See SIFMA letter dated January 27, 2021 (https://www.sec.gov/comments/4-698/4698-8298026-228278.pdf).

ultimately will result in higher costs borne by investors. A number of our members submitted similar letters strongly objecting to the Proposal and urging the Commission to disapprove it.[7]

We also submitted a paper prepared by Professor Craig M. Lewis (the "Lewis Paper") rebutting the points made by the Participants in their Proposal and the CRA Paper.[8] In the Lewis Paper, Professor Lewis concludes that the Proposal would reduce investor welfare by: (1) providing less incentive to the SROs as the operators of the CAT to invest in data security to protect investors' personally identifiable information and trading data in the CAT, which would place investors at greater risk of having their data compromised; and (2) leading to the inefficient purchase of insurance with additional costs likely passed downstream to investors by requiring industry members to absorb litigation-related expenses for an event over which they have no direct control.

On April 1, 2021, the Participants submitted a response to comments ("Participant Response") in which they assert that commenters who oppose the Proposal are asking their primary regulators—the SROs—to bear all liability for hypothetical "black swan" cyber breaches, claiming that such a request is without precedent.[9] The Participants further assert that none of the comments overcome the core premise of the Proposal that the Participants are implementing a regulatory mandate in their regulatory capacities and should therefore receive the liability protections they are customarily afforded when implementing their regulatory responsibilities pursuant to the direction and oversight of the Commission. The Participants also assert that the comments did not offer a sufficient rationale to overcome purported principles regarding allocation of liability between SROs and Industry Members—as memorialized in the Commission-approved rules of securities exchanges and in agreements for national market system ("NMS") facilities and regulatory reporting facilities. In addition, the Participants assert that the comments overlook the Commission's comprehensive oversight of CAT operations, including with respect to cybersecurity, and suggest that commenters are seeking the ability to second-guess the Commission's determinations in court. The Participants also submitted a paper prepared by Charles River Associates on April 5, 2021 responding to and rebutting points made in the Lewis Paper. None of the arguments or submissions of the Participants are persuasive and the Proposal should be rejected for the reasons previously identified by SIFMA.

---

7 See, e.g., Letter from Virtu Financial, Inc. dated January 27, 2021 (https://www.sec.gov/comments/4-698/4698-8298023-228258.pdf); Letter from Raymond James Financial, Inc. dated February 8, 2021 (https://www.sec.gov/comments/4-698/4698-8347733-229000.pdf); Letter from Citadel Securities dated February 23, 2021 (https://www.sec.gov/comments/4-698/4698-8411798-229501.pdf).

8 See Paper from Professor Craig M. Lewis submitted on February 19, 2021 titled "Economic Analysis of Proposed Amendment to National Market System Plan Governing the Consolidated Audit Trail" (https://www.sec.gov/comments/4-698/4698-8394069-229410.pdf).

9 See Participants' letter dated April 1, 2021 (https://www.sec.gov/comments/4-698/4698-8573527-230862.pdf).

II. Discussion

SIFMA consistently has supported the development of the CAT as it will provide a critical market infrastructure resource for regulators to oversee equity and options trading activity across markets. As the Commission has noted many times over the years, the CAT was designed and has been developed as a tool for the Commission and the SROs to use for regulatory purposes only.[10] In this regulatory context, the SROs traditionally have been protected from private liability for any damages they may cause based on the judicially-created doctrine of "regulatory immunity." Despite this broad immunity, the SROs are further seeking to cap their liability through the Proposal in the context of CAT to cover virtually every scenario in which a CAT breach over which they have complete control may cause harm to Industry Members and their customers. Such a further cap is both unnecessary and inappropriate as a matter of public policy, as the SROs already are adequately protected under the existing immunity afforded to them and the grant of further liability protections will allow them to under-invest in CAT cybersecurity measures and insurance protections. We address below the grounds for disapproval of the Proposal under consideration that the Commission included in the Order.

A. Impact of the Proposed Limitation of Liability Provisions on the Incentives of the Participants to Ensure the Security of the CAT and CAT Data

In their response to comments, the Participants insist that the CAT already has robust cybersecurity protections and that *ex-ante* regulation alone of the CAT by the Commission will be sufficient to ensure that the CAT continues to maintain appropriate cyber protections. The Participants note that under the regulatory regime governing the CAT, all interested parties are able to provide feedback to the Commission regarding any Commission proposals addressing the CAT's cybersecurity, including on the Commission's recent proposal designed to enhance the security of data within the CAT System ("CAT Data Security Proposal").[11] The Participants even go so far as to suggest that Industry Members are seeking to second guess the Commission's CAT regulatory decisions in court by seeking the ability to litigate CAT security matters. The arguments are meritless.

At the outset, it is absurd to suggest that SIFMA is questioning the ability of the Commission to effectively oversee and regulate the CAT by seeking to safeguard the ability of Industry Members to recover losses in the event of a CAT Data breach for which the Participants are responsible. We are instead trying to protect our firms from substantial risks that are completely outside of their control. In fact, with regard to Commission oversight of the CAT, we note that the opposite is true, as the Commission recently demonstrated its leadership regarding CAT cybersecurity by issuing the CAT Data Security Proposal. That proposal, which is still pending with the Commission, contains significant enhancements to the security of the

---

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

[11] Id.

CAT System and CAT Data that SIFMA broadly supports.[12] Among other things, it would direct the Participants in the first instance to use Secure Analytical Workspaces ("SAWs") to access and analyze CAT Data obtained through their surveillance queries and any customer and account data. Significantly, it also would define the "Regulatory Staff" at the SROs who have access to CAT Data and would also further clarify the permissible regulatory uses of CAT Data. On this latter point, it would strictly prohibit the use of CAT Data in any commercial context, including in situations in which the data would serve both a surveillance or regulatory purpose, and a commercial purpose (e.g., economic analyses or market structure analyses in support of rule filings).

Despite these commonsense and necessary enhancements to the security of the CAT, the SROs have opposed the Commission's proposal. Certain SROs have objected to the SAW approach in the proposal and argue that they should have the unfettered ability to download CAT Data.[13] They even have argued that the Commission does not have the authority to adopt certain changes in the proposal such as the expansion of FINRA CAT's ability to monitor the use of CAT Data by the SRO Participants.[14] The SROs' opposition to the CAT Data Security Proposal demonstrates the absurdity of their position here. On the one hand, they argue that the Commission's *ex ante* regulation of the CAT is sufficient to ensure that it adopts appropriate security measures, and then on the other, they strongly oppose the Commission when it proposes to do so. Significantly, at the same time the SROs are arguing that the existing CAT cybersecurity protections are adequate, they are completely avoiding responsibility under the Proposal for the consequences of any breach.

While SIFMA fully supports the Commission's regulatory role over the CAT, we note that the regulatory process is complex and takes time and it can sometimes be a year or more before regulatory proposals are adopted by the Commission. Given this pace, it may be difficult for the regulatory process to keep up with the current cyber threat landscape, which is constantly evolving as demonstrated by the recent SolarWinds and Microsoft hacks. Moreover, it is very challenging for Industry Members to gain an understanding of the potential impacts of these or any other hacks on the CAT and the SROs, as well as any security measures they may have adopted in response, given the current cybersecurity requirements for the CAT. While the Commission has proposed to update those requirements in the CAT Data Security Proposal to

---

[12] As the CAT Data Security Proposal is designed to enhance the security and protection of data within the CAT, SIFMA is strongly supportive of that proposal and has encouraged the Commission to swiftly adopt it subject to the Commission's consideration of certain minor enhancements described in our comment letter (https://www.sec.gov/comments/s7-10-20/s71020-8067495-225974.pdf).

[13] See Nasdaq Comment Letter (December 2, 2020), available at https://www.sec.gov/comments/s7-10-20/s71020-8084827-226094.pdf; Cboe Comment Letter (December 2, 2020), available at https://www.sec.gov/comments/s7-10-20/s71020-8088156-226116.pdf; NYSE Comment Letter (December 2, 2020), available at https://www.sec.gov/comments/s7-10-20/s71020-8083358-226075.pdf.

[14] See, e.g., NYSE Comment Letter (December 2, 2020), available at https://www.sec.gov/comments/s7-10-20/s71020-8083358-226075.pdf.

expressly require that corrective actions and breach notifications to CAT Reporters be part of the CAT's cyber incident response plan, the Commission has not adopted that proposal yet. Thus, Industry Members currently are largely in the dark regarding any CAT Data breaches and any remedial measures CAT may adopt in response to them. At a higher level, as discussed further below, Industry Members also generally have little visibility into and input on CAT cybersecurity measures and practices.

In this ever-changing cyber landscape, particularly with this lack of transparency, the CAT and Participants need to be ready to adapt to new cyber threats and practices even in the absence of Commission regulation. Shielding the Participants from any liability to the extent they fail to do so, as the Participants seek to do in the Proposal, clearly is not a reasonable approach. We believe the threat of litigation provides a necessary incentive to the Participants to ensure that they are appropriately adapting CAT security measures to meet new cyber threats.

Similarly, we disagree with the Participants' assertion that the Commission's regulatory regime for the CAT as well as the CAT Advisory Committee provide Industry Members with ample opportunities to weigh in effectively on CAT cybersecurity measures. SIFMA has argued over the years that Industry Members should be made part of the CAT Operating Committee (the governance committee of the CAT) or at minimum CAT Security Working Group to allow them to contribute effectively their cybersecurity expertise to the CAT. Most recently, we argued in response to the Commission's CAT Data Security Proposal that Industry Members should be allowed to become members of the CAT Security Working Group. To date, none of these efforts has been successful and accordingly Industry Members are only afforded limited opportunities to contribute on CAT cybersecurity matters. Tellingly, at the same time the Participants are arguing that the Commission's regulatory process and the CAT Advisory Committee allow Industry Members to weigh-in on CAT security matters, certain Participants are actively seeking to undo through litigation in the D.C. Circuit the only instance in which Industry Members have been given a true say in the operation of a NMS plan by challenging the Commission's order updating the governance of the NMS plans for market data.[15]

B. Existing Regulatory Immunity Applicable to the Participants

The Participants contend that the contractual liability protection provisions they seek to include in the Proposal are the norm for SRO liability protections. They further assert that they are implementing a regulatory mandate in their regulatory capacities and should therefore receive the liability protections they are customarily afforded when implementing their regulatory responsibilities pursuant to the direction and oversight of the Commission. While the SROs' may be implementing a regulatory mandate in their regulatory capacities, we strongly disagree with their view that they need anything more than the judicial doctrine of "regulatory immunity" to protect them in connection with their operation of the CAT to the extent they are acting in a regulatory capacity.

---

[15] See Release No. 34-88827 (May 6, 2020), 85 FR 28702 (May 13, 2020).

Despite Industry Member litigation to the contrary, courts have held for years that an exchange "steps into the shoes" of the Commission with respect to the regulatory functions delegated to it under the Securities Exchange Act of 1934 ("Exchange Act"), and is therefore entitled to broad immunity from private liability with respect to those activities.[16] Courts reason that because the Commission is entitled to sovereign immunity with respect to its own activities, SROs should be entitled to the same immunity when performing quasi-governmental functions that the Commission would otherwise undertake. Although we have not agreed with the broad grants of immunity courts have provided to the SROs over the years, this precedent strongly indicates that courts are likely to view any regulatory activity the SROs conduct through CAT LLC as being subject to this judicial immunity even though it is being conducted in a legal entity that is separate from the SROs.

The Participants also point to the OATS agreement and agreements used in connection with other NMS plans as support for the contractual protections they seek to include in the Proposal. We initially note that these agreements cited by the Participants are frequently those that Industry Members must sign to obtain services such as market data from the SROs, regardless of the liability exclusions contained within them. In any event, the scope of data within the CAT System is exponentially greater than any database that the Participants and Industry Members have ever dealt with before.

As we noted in our January Comment Letter, we believe that the OATS agreement is not an appropriate model for the Proposal because the OATS database contains a fraction of the data that CAT will contain, does not contain customer and account information like CAT, and is limited solely to use by FINRA. On this last point, FINRA, unlike the exchange operators of the CAT, continues to function solely as a self-regulatory organization. On the other hand, the exchanges operate as for-profit corporations that compete with Industry Members and thus are subject to pressures that could cause them to potentially misuse the CAT Data in a commercial manner. Similarly, we believe that other NMS plan agreements with Industry Members, such as the current agreements relating to the NMS plans governing market data, are not appropriate models for the Proposal because the NMS systems relating to the plans contain only a fraction of the CAT Data and do not contain account and customer-level information. The data in these NMS systems does not even come close to having the same level of potential commercial value for the SROs that the CAT Data does.

C. Application of the Proposed Limitation of Liability Provisions to Willful Misconduct, Gross Negligence, Bad Faith or Criminal Acts

---

[16] See, e.g., Barbara v. NYSE, 9 F.3d 49 (2d Cir. 1996) (granting exchange absolute immunity with respect to disciplinary functions); D'Alessio v. NYSE, 258 F.3d 93 (2d Cir. 2001) (extending absolute immunity to exchange's actions in interpreting securities laws); DL Capital v. Nasdaq Stock Market, 409 F.3d 93 (2d Cir. 2005) (finding immunity applied in connection with exchange's alleged delayed announcement of its cancellation of clearly erroneous trades).

The Participants note that even when SRO liability rules permit certain types of claims (e.g., gross negligence and willful misconduct), Industry Members are often prohibited from suing an SRO for damages unless that SRO's alleged gross negligence or willful misconduct also constituted a securities law violation for which Congress authorized a private right of action. They also note that Cboe Rules, which we cited in our January Comment Letter and which provide liability for certain types of conduct such as gross negligence and willful misconduct, are not the norm for SRO liability rules and that most rules in this space do not provide liability for such conduct.

Regardless of whether the Cboe rules are the norm, the overreach of the Participants' Proposal from a policy perspective is fully evident when considering its lack of carve-outs for willful misconduct, gross negligence, bad faith or criminal acts by or on behalf of the Participants. Not only does the lack of such carve-outs deviate from traditional contracting norms, but it also would excuse an exchange or its representatives from liability if they blatantly misused CAT Data for commercial purposes or otherwise committed an outright theft of the CAT Data. For instance, CAT LLC would have only $500 in liability if an SRO employee stole CAT Data and posted it on the internet. This is a particularly egregious outcome, especially considering the CAT costs Industry Members are being asked to pay in the Participants' Proposed Funding Model for the CAT.[17]

One of the biggest concerns Industry Members have with respect to the CAT is the potential that their data and their customers' data in the CAT could be misused, including by SRO insiders. For many types of market participants, access to their transaction data could lead to exposure of their sensitive and proprietary trading strategies and could allow, for example, competitors or bad actors to misuse their data or reverse engineer their trading strategies. Indeed, for certain participants, it is not a stretch to say that they view their trading history with just as much importance as individual investors view their social security numbers. While the SROs would be exposed to enforcement liability if CAT Data is misused or stolen, Industry Members would have no recourse under the Proposal if they suffered a loss arising from the misuse or theft of data, even if data is misused or stolen by an SRO insider. Such an outcome is not only bad policy, but also clearly demonstrates the misalignment of control and liability that we discussed at length in our January Comment Letter.

As we noted, the proposed liability limitation provisions are fundamentally unfair and inappropriate from a policy standpoint. The CAT System is likely to be the largest collection of customer and trading data ever collected and consolidated. It will contain extraordinarily sensitive and proprietary data that must be carefully and aggressively protected against exploitation by hackers and bad actors, as well as misuse for improper competitive purposes. As the repository for virtually all of investors' equity and options trading activity in the United States, the CAT System is an especially attractive target for nation states and other bad actors

---

[17] See Release No. 34-91555 (April 14, 2021), 86 FR 21050 (April 21, 2021).

that have become increasingly sophisticated as the recent SolarWinds hack demonstrates.[18] A CAT data breach could have a devastating impact on market integrity, impose significant harm to market participants and inflict serious competitive harm to Industry Members if their proprietary information is misused or misappropriated. A CAT data breach also could expose those responsible for data contained in the CAT to significant legal risk and potential liability.[19] The sweeping release that the SROs propose would shield them from liability (and allow them to shift liability to individual Industry Members) not only for a breach of the CAT System by malicious third-party actors but even from the theft or other misuse of CAT Data by SRO employees. Such risks are particularly acute in the context of the CAT System, data from which may be accessed by the many hundreds of employees or contractors of 23 separate exchanges and FINRA. Moreover, the Proposal would effectively extinguish the liability of CAT LLC and the SROs even in instances of gross negligence or intentional misconduct by Participants, their employees and agents.

Pursuant to Rule 613 of Regulation NMS and the CAT NMS Plan, CAT LLC and the SROs are responsible for ensuring the security and confidentiality of the information reported to the CAT System. Since the SROs maintain the CAT System, it is entirely inappropriate for the SROs to force Industry Members to assume the additional risks and responsibilities relating to a potential CAT data breach contemplated by the Proposal. The SROs should not be permitted to disclaim liability in the event of a data breach—let alone shift liability risk to Industry Members—when the SROs control the CAT System and are responsible for establishing the information security safeguards designed to prevent a breach.

D. Proposal's Impact on Efficiency, Competition and Capital Formation

As noted in our January Comment Letter and the Lewis Paper, we continue to believe that the Proposal's current allocation of all liability to Industry Members for a CAT Data breach does not promote the Exchange Act goals of efficiency, competition and capital formation because it would ultimately lead to higher costs for investors. The Participants unpersuasively suggest without support that the liability limitation provisions are necessary to ensure the financial stability of the CAT. They assert that CAT LLC has obtained "the maximum extent of cyber-breach insurance coverage," without disclosing any information about the extent or cost of the coverage obtained. It is not at all clear that, to the extent CAT LLC perceives a gap in the insurance coverage, additional insurance could not be obtained.

Moreover, CAT LLC is in a far better position to insure against risks to data under its control, at a much lower cost, than are individual Industry Members. If the liability limitation

---

[18] See https://www.reuters.com/article/us-global-cyber-microsoft/solarwinds-hackers-accessed-microsoft-source-code-the-company-says-idINKBN2951M9.

[19] See, e.g., In re Equifax Inc. Customer Data Security Breach Litigation, No. 1:17-md-2800-TWT, 2020 WL 256132, at *2 (N.D. Ga. Mar. 17, 2020) ($380.5 million payment by Equifax relating to data breach that affected 150 million individuals in United States).

provisions are approved, then every firm submitting data to the CAT System would effectively be forced, where possible, to enhance its individual insurance coverage, at substantial cost, to address the same core risks of data breach or misuse within the CAT System, while at the same time CAT LLC would be permitted to rely on insurance coverage that, by its own admission, is insufficient.

If CAT LLC retains liability associated with CAT Data under its control, then it will be appropriately incentivized to invest in insurance and other risk mitigation measures. Since CAT LLC and the SROs control the CAT System, it is entirely appropriate for them to assume the burden of these investments, without forcing individual firms to fend for themselves and engage in multiple duplicative and overlapping risk mitigation efforts. The ultimate beneficiaries of these efficiencies will be investors in the capital markets.

As Professor Lewis noted in his paper, investors would be at greater risk of having their data compromised under the Proposal since CAT LLC's incentives to invest in security to protect the CAT Data would be reduced. Because Industry Members do not have the ability to directly control the security of the CAT Data, approval of the Proposal in its current form will likely require their purchase of additional liability insurance beyond their existing coverage to address the risk of a breach or misuse of that data. However, requiring Industry Members to absorb litigation-related expenses for a causality over which they have no direct control is inefficient, as they do not have nor can they grant access to insurers to monitor or assess the security of the CAT System. This will result in higher insurance costs, which will ultimately be passed-on to investors.

E. Modifications to the Proposal

The Commission should not approve the Proposal. As we noted in our January Comment Letter, we believe that CAT LLC should be encouraged and incentivized to implement appropriate risk mitigation measures, including supplemental cyber insurance, to cover any potential losses resulting from breach or misuse of CAT Data. The alternative, permitting CAT LLC to disclaim liability pursuant to the Proposal, would effectively require each individual Industry Member to bear liability for data maintained outside of its control by CAT LLC and to pay for and implement separate and overlapping insurance policies, if available, covering the same core risks relating to CAT Data security. This approach is inefficient and would result in substantially higher costs borne by Industry Members and by extension their customers. It would further reduce or eliminate an incentive for the CATLLC and the Participants to ensure robust data security protections are in place.

F. Term Sheet Proposals Attempting to Reach a Resolution

Last year and then again more recently, the SROs approached SIFMA with two proposed term sheets to work toward an amicable resolution of the liability issue – both SRO proposals seek to increase the proposed $500 cap to an aggregate $5,000,000 cap and one of the proposals further seeks to tie compensation for a breach to a future CAT funding model. Under the SROs'

proposals, the higher cap would not be limited to the CAT LLC and Participants acting in a regulatory capacity and thus would give them protections beyond judicial immunity, including if they were to act in a commercial capacity. Furthermore, it is important to note that such a cap would be applied in the aggregate for all CAT data breaches in a calendar year and thus very likely would not make even one firm whole, much less hundreds of firms, for losses that they could incur in connection with a material CAT Data breach. This latter point illustrates why the SROs and Industry Members have not been able to agree on the SROs' proposed cap.

In an attempt to try to reach a resolution with CAT LLC and the Participants, SIFMA provided a revised term sheet proposal to the Participants setting forth the general terms that Industry Members would be willing to discuss with the Participants regarding the allocation of liability in the event of a CAT Data breach. The proposed term sheet builds on and incorporates terms from earlier proposals by CAT LLC and the Participants to SIFMA addressing liability in connection with a CAT Data breach. Specifically, consistent with the regulatory mandate of the CAT, and as discussed at length above, SIFMA proposed that the liability cap should only apply when CAT LLC and the Participants are acting solely in their "Regulatory Capacity." Based on the Commission's further refinement of the concept of regulatory purpose in the CAT Data Security Proposal, Regulatory Capacity would be defined in the term sheet to mean "solely CATLLC, a Participant, or their regulatory staff are performing regulatory functions when using CAT Data, including for market surveillance, investigations, and examinations, and not using CAT Data in such cases where use of CAT Data may serve both a surveillance or regulatory purpose, and a commercial purpose," and "would not include any case where use of CAT Data is for a commercial purpose, or may serve both a surveillance or regulatory purpose, and a commercial purpose (e.g., economic analyses or market structure analyses in support of rule filings submitted to the Commission pursuant to Section 19(b) of the Exchange Act), as the use of CAT Data is not permitted in such cases." We similarly believe that the liability cap should not apply in the event that CAT LLC or the Participants breach the Reporter Agreement or engage in willful misconduct, gross negligence, bad faith or criminal acts.

Again, SIFMA continues to believe that a liability cap is not an appropriate method to address potential CAT data breaches and that CAT LLC and the Participants should be properly incentivized and ensure that they obtain sufficient insurance to cover anticipated losses. However, if Participants believe that a liability cap is necessary despite the judicial immunity already afforded to them, such a cap should be limited to Participants acting solely in a regulatory capacity and should not apply to their commercial activity or where they have breached the contract or have engaged in fraud, willful misconduct or gross negligence.

* * *

SIFMA greatly appreciates the Commission's consideration of our comments above and would be pleased to discuss them in greater detail with the Commission and its Staff. For the reasons discussed above, we strongly urge the Commission not to approve the Proposal in its current form and to encourage CAT LLC to implement appropriate risk mitigation measures, including supplemental cyber insurance, to address any liability arising from breach or misuse of

CAT Data. If you have any questions or need any additional information, please contact me at (212) 313-1287 or egreene@sifma.org.

Sincerely,

Ellen Greene

Ellen Greene
Managing Director
Equity and Options Market Structure

Cc: The Honorable Gary Gensler, Chair
The Honorable Allison Herren Lee, Commissioner
The Honorable Elad L. Roisman, Commissioner
The Honorable Caroline A. Crenshaw, Commissioner
The Honorable Hester M. Peirce, Commissioner

Christian Sabella, Acting Director, Division of Trading and Markets
David Shillman, Associate Director, Division of Trading and Markets
Erika Berg, Special Counsel, Division of Trading and Markets