January 27, 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; Notice of Filing of Amendment to the National Market System Plan Governing the Consolidated Audit Trail by the Plan Participants—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 proposed amendment (the "Proposal") to the National Market System Plan Governing the Consolidated Audit Trail (the "CAT NMS Plan").[2] The Proposal seeks 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.[3] The

[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. 34-90826 (December 30, 2020), 86 FR 591 (January 6, 2021).

[3] 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]."

Proposal would accomplish this by amending the CAT NMS Plan to require Industry Members and their reporting agents each to sign a mandatory agreement as a condition of reporting to the CAT that effectively eliminates the liability of CAT LLC and the SROs in the event of a breach or misuse of CAT Data. [4]

If approved, the Proposal would effectively prevent Industry Members from seeking indemnification, contribution or other relief from CAT LLC and the SROs in connection with claims asserted against Industry Members by customers or others whose data is improperly obtained or misused due to a CAT System security breach. The limitations also could be used to preclude direct claims by Industry Members based on misconduct by CAT LLC, the SROs or their representatives in connection with the CAT System. The Proposal thus would result in fundamentally unfair outcomes and misaligned incentives because it is CAT LLC and the SROs that control the CAT System and the security measures implemented to protect CAT Data.

SIFMA has long supported the development of the CAT and believes that it will provide a critical market infrastructure resource for regulators to track equity and options trading activity across markets. At the same time, SIFMA long has been extremely concerned and vocal about the protection of CAT Data within the CAT System and about the potential liability of Industry Members in the event of a breach or misuse of CAT Data while under the control of the SROs.[5]

For the reasons described below, SIFMA believes 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. 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, the Proposal would allow CAT LLC to under-invest in data security and cyber

[4] 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.

[5] See Letter from Kenneth E. Bentsen, Jr., President and CEO, SIFMA, to the Honorable Jay Clayton, Chairman, Commission, dated June 4, 2020 (https://www.sifma.org/wp-content/uploads/2020/06/SIFMALetter-on-March-17-2020-CAT-Cybersecurity-Questions.pdf).

insurance. This approach is inefficient as a matter of risk mitigation and ultimately will result in higher costs borne by investors in the capital markets.[6]

I. Background

The proposed amendment to the CAT NMS Plan contained in the Proposal is the SROs' most recent attempt to disclaim liability on behalf of CAT LLC for a breach or misuse of CAT Data. In August 2019, CAT LLC's Operating Committee approved a draft Reporter Agreement that included broad limitation of liability provisions substantially similar to those contained in the Proposal.[7] The SROs subsequently refused to permit Industry Members to access to the CAT System, and thereby satisfy their CAT reporting obligations, absent execution of the Reporter Agreement.[8] In response, SIFMA and its members repeatedly voiced their concerns about the Reporter Agreement and its liability limitation provisions. On January 8, 2020, SIFMA proposed an amended version of the Reporter Agreement that, among other things, eliminated the objectionable liability limitation provision.[9]

Despite extensive correspondence and communications between SIFMA and the SROs, the SROs refused to remove the objectionable provisions from the Reporter Agreement and continued to insist on its execution before Industry Members were permitted to access the CAT System to deliver order and trade data. Based on the refusal by the SROs to remove objectionable terms from the Reporter Agreement, certain Industry Members declined to execute the Reporter Agreement. Although other Industry Members executed the Reporter Agreement after the SROs presented it as a condition to obtaining the access to the CAT System necessary to comply with CAT reporting obligations, a number of these Industry Members informed SIFMA that they signed the Reporter Agreement only because they believed they had no other practical choice.

On April 22, 2020, SIFMA filed with the Commission an application pursuant to Sections 19(d) and 19(f) of the Securities Exchange Act of 1934, as amended (the "Exchange Act"), to set aside these actions taken by CAT LLC and the SROs that prohibited or limited SIFMA members with respect to access to the

---

[6] In further support of the comments reflected in this letter, SIFMA will be submitting to the Commission an economic analysis prepared by Professor Craig M. Lewis, former Chief Economist of the Commission, with support from Cornerstone Research.

[7] In particular, Section 5.5 of the proposed Reporter Agreement provided: Limitation of Liability. TO THE EXTENT PERMITTED BY LAW, UNDER NO CIRCUMSTANCES SHALL THE TOTAL LIABILITY OF CAT LLC OR ANY OF ITS REPRESENTATIVES TO CAT REPORTER UNDER THIS AGREEMENT FOR ANY CALENDAR YEAR EXCEED THE LESSER OF THE TOTAL OF THE FEES ACTUALLY PAID BY CAT REPORTER TO CAT LLC FOR THE CALENDAR YEAR IN WHICH THE CLAIM AROSE OR FIVE HUNDRED DOLLARS ($500.00).

[8] The proposed Reporter Agreement itself provided that its execution was a condition of access to the CAT System. It stated: "Whereas, [the Industry Member] desires to access and use the CAT System to comply with its obligations under the CAT NMS Plan, SEC Rule 613 and [SRO] rules, as applicable, . . . CATLLC is making the CAT System available to [the Industry Member] pursuant to the terms and conditions of this [CAT Reporter] Agreement."

[9] See Letter from Ellen Greene, Managing Director, Equity & Options Market Structure, SIFMA, to Michael Simon, CAT NMS Plan Operating Committee Chair, dated January 8, 2020

CAT System in violation of the Exchange Act. SIFMA simultaneously moved for a stay of the SROs' actions in conditioning the submission of CAT Data on executing the Reporter Agreement, or in the alternative, a stay of the impending CAT deadlines. On May 13, 2020, SIFMA and the SROs informed the Commission that the parties had reached a settlement of the proceedings before the Commission and requested that the Commission dismiss SIFMA's application. On May 14, 2020, the Commission granted the parties' dismissal request.

The settlement between SIFMA and the SROs resulted in the removal of the liability limitation provisions from the CAT Reporting Agreements. The Participants now seek to have those same provisions reinserted in the CAT Reporting Agreements pursuant to a CAT NMS Plan amendment. Since Industry Members are required by regulation to submit data to the CAT in accordance with rules approved by the Commission, the result of the Proposal would be to compel Industry Members involuntarily to absorb contractually all of the risk associated with meeting their regulatory requirements, while excusing CAT LLC and the SROs from any responsibility associated with losses caused by a breach or misuse of CAT Data within the CAT System controlled and managed by CAT LLC and the SROs. In other words, the Proposal seeks to impose by regulation mandatory contractual provisions that are harmful to Industry Members, unfair and inconsistent with good public policy.

II. Discussion

The Participants' proposal to add sweeping liability limitation provisions to the CAT Reporting Agreements is based on flawed arguments that are fundamentally in conflict with one another. On the one hand, the Participants assert that Industry Members should not be concerned about breach or misuse of CAT Data because of the robust regulatory regime governing CAT data security; on the other hand, they argue that the risk of a catastrophic loss as a result of a data breach or misuse is so significant that the financial stability of the CAT would be jeopardized in the absence of the liability limitation provisions. Their proposed amendment would excuse CAT LLC and the SROs entirely in the event of a breach or misuse of data exclusively within their control, and would assign the liability risk to Industry Members for potentially catastrophic losses caused by security failures entirely outside of their control.

The guiding principle in this context should be that the party in control of the CAT System—CAT LLC—must assume liability for any failure to maintain CAT data security. Aligning control and liability is not only fair and equitable; it is also good policy, because it maximizes efficiencies in managing data risks inherent in the CAT System.

As discussed below, 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.

A. The Proposed Liability Limitation Provisions are Fundamentally Unfair and Inappropriate as a Policy Matter

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 that have become increasingly sophisticated as the recent SolarWinds hack demonstrates.[10] 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 the CAT and data contained in the CAT to significant legal risk and potential liability.[11] 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.

These risks are magnified to the extent that the SROs are permitted to engage in bulk downloads of CAT Data. Any of the SROs that jointly operate the CAT currently may download onto their servers vast amounts of customer and trading data, thus multiplying the sources of a potential data breach and increasing the risk that data is misappropriated, misused or lost.[12] As discussed below, the Commission has recognized the risks associated with bulk downloading and proposed limitations on bulk downloads of

---

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

[11] 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).

[12] SIFMA members have long expressed particular concern about the need to protect personally identifiable information ("PII") of individual customers. See, e.g., Letter from Thomas Price, Managing Director, SIFMA to Brett Redfearn, Director, Division of Trading and Markets, SEC dated October 29, 2018; SIFMA White Paper titled "Consolidated Audit Trail – Alternative Approach for the Collection of Investor Personally Identifiable Information Leveraging the CAT Customer Identifier (CCID)" dated October 29, 2018; Letter from Thomas Price, Managing Director, and Ellen Greene, Managing Director, SIFMA to Jon Kroeper, EVP, FINRA dated August 13, 2018.

CAT Data, and yet the SROs have resisted these limitations designed to increase CAT data security while urging the Commission at the same time to eliminate their liability. The risks and uncertainties related to CAT Data are further increased since the SROs are in the process of finalizing the scope of the customer identifying information to be reported to and maintain by the CAT through the CAT Customer and Account Information System specification.

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.

The protection of the data in the CAT System is of paramount importance not only to Industry Members, but also the Commission itself. As former Chairman Clayton observed, "the SROs must be mindful of the volume of data that the CAT collects, and its sensitive nature, and be responsible in their collection and use of that data" as "the nature of the data to be included in the CAT necessitates robust security protections." Indeed, the Commission issued a proposal in August 2020 designed to enhance the security of data within the CAT System ("CAT Data Security Proposal") that is still pending with the Commission.[13] The CAT Data Security Proposal contains many of the recommendations that SIFMA and others have made over the years to enhance the security and protection of CAT Data.

The Proposal is even more inappropriate in light of the commentary submitted by the SROs in response to the CAT Data Security Proposal.[14] The Plan Operating Committee Chair and several of the Participants have submitted comment letters opposing the CAT Data Security Proposal.[15] These letters maintain that the current security profile of the CAT already is sufficiently robust and that the Commission's proposed

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

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

[15] See Michael Simon Comment Letter (December 4, 2020), available at https://www.sec.gov/comments/s7-10-20/s71020-8100247-226195.pdf; FINRA CAT Comment Letter (December 2, 2020), available at https://www.sec.gov/comments/s7-10-20/s71020-8088162-226120.pdf; 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.

enhancements will result in undue costs and delay in implementing and operating the CAT.[16] Among other things, the Participants take issue with the proposed Secure Analytical Workspace ("SAW") approach to conducting surveillance activities and with the proposed limits on bulk downloading of CAT Data.[17] For the Participants to argue against the adoption of the CAT Data Security Proposal while at the same time attempting to disclaim all liability associated with CAT Data is not only disingenuous, it is dangerous and underscores the policy risks of de-linking control and liability. It is self-evident that without any liability whatsoever with respect to CAT data security, CAT LLC would not be sufficiently incentivized to implement the necessary data security and risk mitigation measures.

B. The Proposed Liability Provisions are Inconsistent with Industry Standards

The Participants further argue that the proposed liability provisions are dictated by "industry norms" and suggest that these provisions are an essential element of the self-regulatory framework, referencing a number of existing exchange rules that limit SRO liability. These arguments mischaracterize entirely the referenced rules and their applicability. In fact, the referenced exchange rules actually provide for SRO liability in a variety of circumstances.

For example, Rule 1.10 of the Cboe Exchange, Inc. imposes SRO liability arising from the "willful misconduct, gross negligence, bad faith or fraudulent or criminal acts of the Exchange or its officers, employees or agents[.]" Rule 527 of the Miami International Securities Exchange, LLC likewise imposes SRO liability for willful misconduct and gross negligence on the part of the exchange, its officers, employees, or agents. Indeed, each and every exchange rule referenced by the Participants in this connection provides for SRO liability.[18] These exchange rules, if anything, demonstrate that the liability limitation provisions in the Proposal are completely out of line with industry standards. At the very least,

---

[16] See, e.g., Michael Simon Comment Letter (December 4, 2020), at 3 ("The Participants believe . . . that a robust security system has been developed and implemented for the CAT"); Cboe Comment Letter (December 2, 2020), at 6 (The existence of [the Cboe Exchanges'] security protocols . . . makes it unnecessary for the Commission to impose the additional restrictions in the Proposal.")

[17] Michael Simon Comment Letter (December 4, 2020), at 4-5; Nasdaq Comment Letter (December 2, 2020), at 9; Cboe Comment Letter (December 2, 2020), at 5.

[18] See Nasdaq GEMX, Section 27(a) (authorizing the Exchange to "compensate users of the Exchange for losses directly resulting from the actual failure of the System, or any other Exchange quotation, transaction, reporting, execution, order routing or other systems or facility to correctly process an order, quote, message, or other data"); NYSE, LLC Rules 17 and 18 (authorizing the Exchange to "make a payment to the claiming member organization for the claimed losses on the amounts," establish a "Compensation Review Panel" to determine the precise amount to be paid, and authorizing lawsuits against third-party vendors in certain instances); Investors Exchange, Rule 11.260 and Long-Term Stock Exchange, Rule 11.260 (authorizing compensation "for losses directly resulting from the Systems' actual failure to correctly process an order, message, or other data"); BOX Exchange LLC, Rule 7230 (authorizing compensation by the Exchange for "losses resulting directly from the malfunction of the physical equipment, devices, or programming of Exchange Related Persons and/or Entities, or from the negligent acts or omissions of employees of the Exchange or BOX"); Nasdaq, Rule 4626 (authorizing compensation by the Exchange "for losses directly resulting from the systems' actual failure to correctly process an order, Quote/Order, message, or other data").

liability limitations should not extend to willful misconduct, gross negligence, bad faith or criminal acts of CAT LLC, the SROs or their representatives or employees.

The Participants also cite OATS as an example of an audit trail system that requires Industry Members to agree to liability limitation. This comparison is baseless, however, as the CAT provides unprecedented and unfettered access by every SRO to trading data on every platform. OATS was created two decades ago, before fundamental changes in data privacy and cybersecurity. OATS captures only a fraction of the data that the CAT will contain. For example, OATS does not contain market maker orders, customer identifying information, or any information regarding options orders or executions. Similarly, OATS lacks account-level data that presents the risk of reverse engineering trading strategies using OATS data. The CAT System, by contrast, will capture significantly more information, making it a much more attractive target for hackers. In addition, OATS data is reported to FINRA and used by FINRA alone. CAT Data, by contrast, will be reported to 24 different SROs and accessible by personnel at each of those SROs. The potential for a data breach is exponentially greater in the CAT context.

Finally, it is important to remember that the SROs have long asserted and, indeed, have received from the courts immunity from liability in circumstances where they are acting in a regulatory capacity.[19] The SROs fail to explain why further limitation of their liability should be imposed by contract. Their effort to do so raises significant questions about whether the SROs seek to avoid liability in circumstances in which they misuse CAT Data while acting in a commercial capacity where they might not otherwise be entitled to regulatory immunity.

C. The Proposed Liability Limitation Provisions are not Necessary to Ensure the Financial Stability of the CAT

The Participants misleadingly suggest 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 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.

[19] See, e.g., DL Capital v. Nasdaq Stock Market, 409 F.3d 93 (2d Cir. 2005).

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.

D. The Participants' Economic Analysis is Fundamentally Flawed

The Participants have submitted a lengthy report prepared by Charles River Associates (the "CRA Report") that purports to be an analysis of economic issues relating to the cyber security of the CAT. The CRA Report is flawed in numerous respects.

The CRA Report is fundamentally erroneous in framing the issues for the Commission's consideration. The first analysis presented is an assessment of the likelihood and severity of various potential breach scenarios involving CAT data. The analysis focuses only on breach by external actors and fails to address at all the risk of misuse of CAT data by personnel at CAT LLC and the SROs who have access to the data, a critical omission given that the SROs propose to extinguish their liability for the misuse of CAT data even by their own employees.

The second analysis focuses on whether the risk of a cyber-breach of the CAT should be addressed through ex ante regulation or ex post litigation or a combination of both approaches. CRA incorrectly suggests that the Commission has a choice between regulating the CAT (which it is already doing) and imposing litigation liability with respect to the breach or misuse of CAT Data. That is a false choice because the risk of breach or misuse of CAT Data is already subject to an ex post litigation by virtue of the fact that Industry Members can themselves be sued for data security failures in the CAT System. Industry Members do not have the choice to simply disclaim liability and adopt a "regulatory regime" based on a white paper.

A central conclusion of the CRA Report is that the risk of a cyber-breach of the CAT should be addressed through an ex ante regulatory approach rather than an ex post litigation approach or a combination of both approaches. In reaching this conclusion, CRA argues that the costs of litigation to CAT LLC (and by extension the Participants and Industry Members that fund CAT LLC) are high, and that the expected benefits are low, and therefore that "there is no economic justification for allowing additional litigation." Incredibly, CRA suggests that additional investment in CAT Data security—so-called "extra-marginal defensive investments in cyber risk protection"—would not be economically justified.

Again, CRA only considers part of the equation. The flaw in CRA's argument is that it 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. Disclaiming liability by CAT LLC no doubt would reduce costs of CAT LLC

itself—but the corollary missing from the CRA Report is that the liability for a potentially catastrophic loss would then be shifted to individual Industry Members. For the firm whose data happens to be hacked while under the control of CAT LLC, the "regulatory regime" is anything but economically justified.

The final section of the CRA Report provides "thoughts on funding compensation mechanisms" that appear to contradict certain assertions made by the Participants in the Proposal. While CRA contends that ex ante regulation offers a supposedly better course for addressing the risk of a breach or misuse of CAT data, CRA acknowledges that the existing regulatory regime in fact does not currently address the underlying problem. CRA concedes that the "current regulatory approach is generally silent on the possibility of compensating third parties in the case of a CAT cyber breach." Because the regulatory regime is silent on how injured parties would be compensated in the event of a CAT breach, CRA proposes "initial thoughts" on "funding compensation mechanisms" that CAT LLC and the Commission "could consider" after "a careful evaluation of the costs, benefits, and incentives among the various parties associated with the CAT." Neither CAT LLC nor the Participants actually propose the adoption of any of these regulatory mechanisms to fill the gap in the regulatory approach that CRA identifies. Should the liability of CAT LLC and the Participants be extinguished, they of course will have no incentive to develop any mechanisms for compensating third parties injured if the CAT System is breached or CAT Data is misused while under the control of CAT LLC and the SROs. The SROs thus urge the Commission to extinguish their liability in favor of a regulatory approach but concede that the current regulatory regime, without more, is insufficient to protect parties injured as a result of a CAT data breach.

As noted above, the Participants assert that they have no choice but to disclaim liability because that CAT LLC has obtained the "maximum extent of cyber-breach insurance coverage available" and such insurance is insufficient to protect the Participants from associated risks. The CRA Report, however, suggests that additional cyber insurance could be used to address catastrophic "black swan" events and that other financial tools, such as industry loss warranties or catastrophe bonds, could be used to supplement traditional insurance.

We agree that insurance products, potentially coupled with other financial tools, are a critical component of managing risks associated with CAT Data. We also agree with the implication in the CRA Report that insurance against risks associated with CAT Data can be most efficiently obtained in a centralized manner by CAT LLC itself. If the Proposal is approved, CAT LLC would have no incentive to pursue more robust insurance protection because it would have no litigation exposure. Individual firms would separately be forced to seek and pay for duplicative and overlapping insurance products to protect against a risk that is entirely out of their control. CRA rightly notes that cyber coverage entails a high degree of monitoring, and it is far from clear that individual firms could offer monitoring of the CAT System sufficient to obtain appropriate levels of insurance. More fundamentally, it is far more efficient and equitable for CAT LLC to bear responsibility for insuring against a CAT data breach than it is for every

Industry Member to be forced to fend for themselves, particularly where CAT LLC and the SROs control the CAT System and are responsible for securing the CAT System.

* * *

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 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 [redacted] or [redacted].

Sincerely,

Ellen Greene
Managing Director
Equity and Options Market Structure

Cc: The Honorable Allison Herren Lee, Acting Chair
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
Erika Berg, Special Counsel, Division of Trading and Markets