CRA Charles River Associates

CRA Response to:

Economic Analysis of Proposed Amendment to National Market System Plan Governing the Consolidated Audit Trail

by
Craig M. Lewis, Ph.D.

and

Selected Points in Public Comment Letters

Date: April 5, 2021

Table of Contents

I. Introduction

On December 18, 2020, the participants (the "Participants") in the National Market System Plan Governing the Consolidated Audit Trail (the "CAT NMS Plan" or "Plan") proposed an amendment (the "Proposed Amendment") to the Plan authorizing Consolidated Audit Trail, LLC ("CAT LLC") to revise the Consolidated Audit Trail Reporter Agreement (the "Reporter Agreement") and the Consolidated Audit Trail Reporting Agent Agreement (the "Reporting Agent Agreement," collectively the "CAT Reporting Agreements") to include limitation of liability provisions. Counsel for the Participants engaged Charles River Associates ("CRA")[1] to conduct an independent economic analysis of the Proposed Amendment, which was memorialized in a white paper (the "CRA White Paper") entitled *Analysis of Economic Issues Attending the Cyber Security of the Consolidated Audit Trail*. At a high level, the CRA analysis concluded that a limitation on liability would serve the public interest by facilitating the regulation of the U.S. equity and option markets at lower overall costs and higher economic efficacy. CRA further concluded that CAT's cyber risk should be addressed through the regulatory approach that the SEC has already adopted, and that giving Industry Members the right to sue for monetary damages should they suffer losses due to a CAT cyber breach would decrease social welfare.

The Proposed Amendment has generated opposition from certain Industry Members that would sign the proposed amended CAT Reporting Agreements, and their trade associations, including the Securities Industry and Financial Markets Association ("SIFMA"). On February 19, 2021, SIFMA submitted a report prepared by Professor Craig M. Lewis of Vanderbilt University (the "Lewis Report").[2] Lewis disagreed with the analysis presented in the CRA White Paper and concluded "that the proposed amendment, if adopted, would result in a reduction in investor welfare.[3]

Counsel for the Participants has asked us to respond to the Lewis Report and address industry comments to the extent they implicate economic issues. In general, Lewis's analysis (and related comments from Industry Members) suffers from several fundamental flaws:

- In concluding that providing Industry Members the right to litigate against CAT LLC, the Participants, and FINRA CAT for damages is necessary to properly incentivize the Participants to take appropriate cyber security precautions, Lewis ignores other incentives, such as the substantial incentives created by the SEC's existing regulatory regime and the risk of reputational harm to various CAT stakeholders (including the SEC) and third party vendors (among other sources of incentives) with whom CAT engages who have the ability to influence the cyber program at CAT;
- In concluding that providing Industry Members the right to litigate against CAT LLC, the Participants, and FINRA CAT for damages is necessary to properly incentivize

---

1 The identification and qualifications of CRA's authors / principal investigators for the original CRA White Paper and this Response were presented in Section V of the CRA White Paper.

2 See Letter from Ellen Greene, Managing Director, Equity and Options Market Structure, SIFMA to Vanessa Countryman, Secretary, SEC, February 19, 2021.

3 Lewis Report ¶ 38.

the Participants to take appropriate cyber security precautions, Lewis ignores that because the Commission has approved joint funding of CAT LLC by Industry Members and the Participants, a limitation of liability also protects Industry Members from the possibility of funding both catastrophic losses and substantial litigation costs;

- Lewis (and commenters) fail to acknowledge that Industry Members have been provided multiple methods to monitor and influence the CAT's cyber security including by participating on the Advisory Committee, commenting on the SEC's proposed cyber requirements for the CAT, and petitioning the Commission for rulemaking directly;
- Lewis (and commenters) fail to acknowledge that providing Industry Members the right to litigate for damages may have the unintended consequence of reducing Industry Members' incentives to undertake their monitoring and influencing activities in favor of relying upon the threat of litigation—a threat that we have already established provides weak incentives to alleviate risk—thereby weakening the overall cyber program at the CAT; and
- Lewis's argument that CAT LLC is in a better position than Industry Members to insure against a CAT Data breach fails because (among other reasons) it is based on Lewis's incorrect premise that a cyber breach would necessarily impact all Industry Members simultaneously and ignores the fact that CAT LLC has already purchased the maximum insurance coverage that was feasibly available at the time.

After reviewing the Lewis Report and comment letters, we maintain our conclusion that combining the Commission's existing regulatory regime with a limitation of liability is the most efficient manner of addressing the complex issues presented by a potential CAT Data breach.

II. Summary of CRA's Responses to Lewis Report

This section summarizes Lewis's principal opinions, identifies economic issues raised by comment letters, and provides an overview of CRA's responses. Lewis's principal conclusion is that the proposed limitation of liability would increase the risk of investor harm and costs posed by a potential CAT breach. Based on that conclusion, Lewis argues that forcing CAT LLC to internalize the potential costs from all parties conceivably affected by a breach would lead to the most economically efficient outcome.[4] We address these arguments (among other issues) below.

A. The SEC's Regulatory Regime

As an overarching matter, much of Lewis's analysis seems to be based on an erroneous premise—namely, that CAT LLC would avoid all liability arising from a potential CAT breach if the Commission approves the proposed limitation of liability. Contrary to Lewis's premise, the limitation of liability provisions bind only signatories to the CAT Reporter Agreements—Industry Members and the Participants—not the Commission itself (or any other parties). As a result, the Commission would retain its ability to address CAT Data security through *ex-ante*

[4] Lewis Report ¶ 3.

regulation and *ex-post* enforcement action if the Commission approves the Proposed Amendment. Most of Lewis's conclusions fail for this reason alone.

Relatedly, Lewis also errs by assuming that the SEC's regulatory regime for the CAT—backed by the Commission's enforcement function—is essentially useless in aligning the incentives of the various stakeholders of CAT LLC regarding cyber security, including Industry Members. In particular, Lewis overlooks the cyber security requirements in the Plan and subsequent Plan modifications to ensure the CAT's security. Indeed, the SEC itself concluded that its cyber security regulations serve the public interest, especially when considered in the context of its overall regulatory mandate to protect the efficient and fair functioning of the U.S. securities markets.[5] Lewis's premise seems to be that Industry Members need the ability to second guess the Commission's CAT oversight and enforcement decisions in court.

Lewis also fails to consider another fundamental aspect of the applicable regulatory regime—the Commission's inspection and examination authority. CAT LLC's, FINRA CAT's and the Participants' compliance with the Commission's cyber security mandates is subject to review by the Division of Examinations on both a cyclical and for-cause basis. Moreover, the Commission's cyber security personnel—including its Chief Information Officer—are able to assist the Commission (and its staff) in evaluating any potential enhancements to the CAT's cyber security.

The CRA White Paper summarized the SEC's regulatory requirements for CAT cyber security and provided detailed references to underlying documents that were reviewed in the process of developing the analysis. The Lewis Report did not reference—let alone examine—those documents that, in our opinion, are necessary to understand the actual circumstances attending the CAT's cyber security.

Lewis also ignores that, as part of the Commission's regulatory structure, Industry Members have a voice in the oversight and operations of the CAT through their participation in the Advisory Committee. Contrary to the position of Lewis and several commenters, Industry Members and other interested parties are able to monitor and suggest improvements for the CAT's cyber security. The history is replete with examples of Industry Members influencing CAT's cyber security, including with respect to:

- the initial approval of the plan by the SEC on November 15, 2016;[6]
- the March 17, 2020 "Order Granting Conditional Exemptive Relief" for handling customer and account information;[7] and

---

5 The SEC noted "that it agrees that the CAT Data will be a particularly attractive target for bad actors. However, the Commission believes that the extensive, robust security requirements in the adopted Plan, as outlined in Section IV.D.6, provide appropriate, adequate protection for the CAT Data." Securities and Exchange Commission, *Joint Industry Plan; Order Approving the National Market System Plan Governing the Consolidated Audit Trail*, Release No. 34-79318, November 15, 2016, hereafter "SEC, *Order Approving CAT,*" Section V.F.4, p. 715.

6 SEC, *Order Approving CAT.*

7 Securities and Exchange Commission, *Order Granting Conditional Exemptive Relief, Pursuant to Section 36 and Rule 608(e) of the Securities Exchange Act of 1934, from Section 6.4(d)(ii)(C) and Appendix D Sections 4.1.6, 6.2, 8.1.1, 8.2, 9.1, 9.2, 9.4, 10.1, and 10.3 of the National Market System Plan Governing the Consolidated Audit Trail*, Release No. 34-88393, March 17, 2020.

- the May 15, 2020 "Amendments to the National Market System Plain Governing the Consolidated Audit Trail" (focusing on "public transparency requirements").[8]

We also note, as another example of Industry Members' ability to influence the CAT's cyber security, Industry Members and SIFMA are able to meet directly with Commissioners and the Commission's Senior Officers.[9]

B. Optimal Incentives to Protect CAT Data

Lewis's analysis concludes, without support, that the absence of a limitation on liability provision in the CAT Reporter Agreements would meaningfully improve CAT LLC's incentives to take appropriate cyber security precautions compared to the current framework. That conclusion is not credible. It is important to recognize that there is presently no asset reserve on the balance sheet of CAT LLC sufficient to cover a substantial cyber loss. Therefore, adding the threat of litigation from Industry Members may not provide any additional incentives to invest in preventive care. Industry Members' ability to monitor the CAT's cyber security program through their participation on the Advisory Committee, however, provides an alternative way for this stakeholder group to ensure that the Participants take appropriate precautions.

To the extent litigation can provide incentives to take additional precautions here, the limitation of liability does not restrict the SEC's ability to bring enforcement actions. The SEC's regulatory framework—which includes the Commission's enforcement function—already provides appropriate incentives for the Participants, CAT LLC, and FINRA CAT to invest in cyber security at levels that reflect the considered interests of all parties interested in the fair and efficient functioning of U.S. securities markets.

We also note the considerable reputational harm that would befall CAT LLC, the Participants, FINRA CAT, cyber security vendors to the CAT, and the SEC itself in the event of a cyber breach. Two of those stakeholders (i.e., CAT's vendors and the SEC) also have the ability to monitor CAT's effort to take appropriate precautions. The vendors can make proposals and try to impose obligations through contract negotiations and use their specialized knowledge and unique access to CAT operations to give advice to the managers about possible improvements to CAT operations. Lewis and the commenters generally ignore these incentives for the Participants, CAT LLC, FINRA CAT, and other interested parties to maintain vigilance with respect to the CAT's investments in cyber security. As discussed in the CRA White Paper, these incentives are sufficient to ensure that the Participants, FINRA CAT, and CAT LLC will invest at levels that reflect the interests of all potentially affected parties in the CAT's cyber security—including Industry Members.

C. Insurance Considerations

Lewis also comments on the purchase of cyber liability insurance by CAT LLC and by Industry Members. Lewis's insurance analysis fails in large part because it is based on the same erroneous premise that the limitation of liability provisions in the Proposed Amendment allow

---

[8] Securities and Exchange Commission, *Amendments to the National Market System Plan Governing the Consolidated Audit Trail*, RIN 3235-AM60, Release No. 34-88890, File No. S7-13-19, May 15, 2020.

[9] For a recent example, see *Meeting with Representatives of SIFMA*, File Nos. S7-10-20; 4-698 at https://www.sec.gov/comments/s7-10-20/s71020-8400451-229460.pdf, accessed April 2021.

CAT LLC, FINRA CAT, and the Participants to avoid all liability in the event of a cyber breach. Again, this is not true. In fact, if it were true, there would be no need to purchase cyber insurance at all (which could cover, among other things, costs associated with regulatory investigations).

Relatedly, Lewis asserts, without evidence or substantive analysis, that CAT LLC would purchase additional insurance if limitation of liability provisions were not included in the CAT Reporter Agreements. Indeed, his economic conclusion that investor welfare would be enhanced by the absence of limitations of liability in the CAT Report Agreements depends largely, if not entirely, on the propositions that: 1) CAT LLC can purchase additional and more targeted cyber insurance in an attempt to pre-finance possible cyber claims from Industry Members and 2) Industry Members would experience a corresponding decrease in their cyber security risks and insurance rates more than commensurate to the increase in CAT LLC's cyber insurance rates. We are not aware of any basis for those assertions (nor does Lewis offer any).

Fundamental to Lewis's insurance analysis is his erroneous assertion that the limitation of liability provisions will force claims onto Industry Members from their clients and financially burden Industry Members with purchasing additional insurance coverage. He does not explain how Industry Members' clients can sue Industry Members for a cyber breach at the CAT, nor does Lewis consider the fact that many Industry Members have limitation of liability provisions in their respective customer agreements. Finally, Lewis does not explain how an insurer would write liability coverage for Industry Members paying claims to their clients for an adverse cyber event at the CAT.

III. Background and Implications of Proposed Amendment

In this section, we respond to Lewis's discussion of certain background and contextual considerations that inform the economic analysis of the Proposed Amendment.

The Lewis Report begins with an account of the structure of the CAT. In that discussion, he claims that "[a]fter reporting its data to CAT LLC, Industry Members have no control over the security of the data and bear **no responsibility for its safekeeping**."[10] This statement ignores the significant ability Industry Members have been granted through the SEC's overall regulatory structure to influence the CAT's cyber security program. We discuss this point in detail in Section IV.

Lewis notes that "it appears that the SEC was sufficiently concerned about data security that it proposed amendments to the CAT NMS Plan in August 2020 that removed the collection of certain sensitive PII (such as social security numbers and date of birth) and included further security requirements."[11] The Citadel public comment letter similarly states that "the Commission in August 2020 proposed enhancements to the security of CAT data, which included proposed amendments to the CAT NMS Plan designed to improve the security of CAT data that is extracted from the CAT by a Participant."[12] Neither the Lewis Report nor the Citadel

[10] Lewis Report ¶ 7, emphasis in original.
[11] Lewis Report ¶ 8.
[12] Letter from Stephen John Berger, Managing Director, Global Head of Government & Regulatory Policy, Citadel Securities to Vanessa Countryman, Secretary, SEC, February 23, 2021, p. 2, hereafter "Citadel."

comment letter, however, acknowledge the implications of the SEC's August 2020 actions (and other actions) from the perspective of economic analysis. As discussed in detail in the CRA White Paper, these actions highlight the active role of the SEC in regulating the CAT. This demonstrates that the *ex-ante* regulatory approach is working exactly as intended, and that adding *ex-post* litigation by Industry Members is unnecessary to yield incremental improvements in the CAT's cyber program and it would needlessly increase expected costs.

It is notable that Lewis does not acknowledge the contents or even the existence of relevant documents, practices, and protocols including: 1) Appendix D to the Plan, which describes the cyber security requirements mandated for the CAT, 2) the SEC's oversight role including as a permanent observer on the Operating Committee, 3) the mandatory participation of Industry Members and other representatives of the investing public on the Advisory Committee, and 4) other cyber security considerations implemented at the behest of the SEC or Industry Members or by CAT LLC itself. Similarly, while Lewis extensively quotes the portions of the CRA White Paper discussing the general features of the CAT, he ignores CRA's analysis regarding the CAT's cyber security infrastructure (including regulatory requirements) and analyzes the CAT's cyber security as if it would be nonexistent without the ability of Industry Members to litigate for monetary damages. CRA's White Paper contained an eight-page description of the Research Program and Bibliography listing the documents that provide additional detail on the CAT's cyber security practices and protocols, the SEC's role in cyber security attending the CAT, and changes implemented to improve cyber security.

The last two paragraphs of Section II of the Lewis Report present his "implications," which are foundational to the rest of his analyses. In substance, Lewis asserts that the Proposed Amendment would force Industry Members to assume liability for all breaches, and, in the event of a breach, Industry Members would face claims from their underlying clients, without any ability to control risk or efficiently purchase cyber insurance.[13] Lewis's assertion can be found, in some cases almost verbatim, in several comment letters.[14]

There are at least three analytical weaknesses in Lewis's assessment of the "implications" of including the limitation of liability provisions in the CAT Reporter Agreements. First, Lewis disregards the potential for enforcement action by the SEC against the Participants. The CAT is an entity mandated by the SEC to help it regulate U.S. financial markets. The SEC has substantial enforcement capabilities and conducts substantial regulatory oversight of the CAT. Lewis does not provide any reason to doubt the willingness or ability of the SEC to exercise its authority over CAT cyber security. It is worth reiterating that the law and economics literature, cited extensively in the CRA White Paper, demonstrates that *ex-ante* regulation can more efficiently motivate appropriate levels of investments in safety than *ex-post* liability for damages

[13] Lewis Report ¶¶ 9-10.

[14] Letter from Ellen Greene, Managing Director, Equity and Options Market Structure, SIFMA to Vanessa Countryman, Secretary, SEC, January 27, 2021, pp. 1-2, hereafter "SIFMA"; Letter from Matthew Price, Chief Operations Officer, Fidelity Capital Markets National Financial Services LLC to Vanessa Countryman, Secretary, SEC, February 2, 2021, p. 2; Letter from Thomas R. Tremaine, Executive Vice President, Chief Operations Officer, Raymond James & Associates, Inc. to Vanessa Countryman, Secretary, SEC, February 8, 2021, p. 2, hereafter "Raymond James"; Letter from Daniel Keegan, Managing Director, Head of North America Markets & Securities Services, Citigroup Global Markets, Inc. to Vanessa Countryman, Secretary, SEC, February 25, 2021, p. 1, hereafter, "Citigroup."

when a loss occurs as applied to the circumstances and context that are associated with the CAT and its potential cyber security exposure. We discuss this point in further detail in Section IV.

Second, Lewis's analysis proceeds as if it is self-evident that the overall benefits of allowing Industry Members to recover damages against CAT LLC and the Participants could exceed the costs of allowing such litigation when the SEC's regulatory regime and the reputational concern of CAT LLC, FINRA CAT, the Participants, the CAT's cyber security vendors, and the SEC itself already work to ensure a high level of cyber security for the CAT. As discussed in the CRA White Paper, litigation can effectively incent *ex-ante* actions to reduce risk in the absence of the regulatory and reputational concerns; but regulation and reputational considerations can also motivate appropriate *ex-ante* actions to reduce risk. There is no recognition of this economic principle in Lewis's analysis.

Third, Lewis claims that, in the event of a CAT breach, "Industry Members would likely be the subject of claims by their clients and sued as a result of any damages suffered by those whose data were compromised."[15] Lewis offers no basis for this conclusion, and it is not clear how Industry Members could be held liable for a cyber breach at the CAT, particularly in light of the limitations of liability that Industry Members often impose upon their own customers. As a result, core elements of Lewis's analyses rest on unsubstantiated speculation.

IV. Economic Analysis of the Proposed Amendment

Lewis opines that investors would be harmed by the proposed amendment for two reasons. First, the Proposed Amendment would result in a higher likelihood of a cyber breach because CAT LLC would not face litigation threat sufficient to prompt it to adequately safeguard data. Second, the overall cost of cyber insurance for parties participating in the CAT (the Participants and Industry Members) would be higher because Industry Members would have to purchase insurance for events over which they have no control.[16]

Lewis's conclusions fail because they rely on premises that are false or inapplicable to the CAT. Among other issues, Lewis:

- Ignores the binding mandates of the SEC that serve to align the cyber security interests of CAT LLC with the SEC's goal of protecting the investing public, as well as the SEC's ongoing ability to address CAT security issues in a manner specifically tailored to the CAT through *ex-ante* regulation and *ex-post* enforcement action;[17]
- Disregards the unique governance structure that provides Industry Members access to information about the operations of the CAT and the ability of Industry Members to influence cyber security, on an *ex-ante* basis, of CAT Data;
- Fails to acknowledge that providing Industry Members with an *ex-post* right to litigate for damages may do little to incentivize CAT management to invest further in cyber protection beyond the regulatory structure already in place and, in fact, may increase the risk of a future event if allowing Industry Members to seek

[15] Lewis Report ¶ 10.
[16] Lewis Report ¶ 11.
[17] CRA White Paper, Section III.

damages against the Participants reduces the incentives of Industry Members to exercise their *ex-ante* influence through their active participation on the Advisory Committee;

- Fails to acknowledge that allowing Industry Members to litigate against CAT LLC and the Participants for damages entails potentially substantial costs and uncertainty in the operation of the CAT that, ultimately, could be borne by Industry Members' underlying customers;
- Neglects the interests that CAT LLC, the Participants, the technology vendors to the CAT, and the SEC have in avoiding the damage to their reputations that would result from a cyber breach, and the ability of each of these parties to incentivize, on an *ex-ante* basis, CAT managers to take precautions to avoid a cyber breach; and
- Demonstrates a superficial understanding of insurance issues in relation to CAT LLC, Industry Members, and the investing public.

A. Alignment of Control and Liability, Incentives for the Optimal Amount of Data Security, and Benefits to Investors

Lewis's economic analysis begins with an assertion that the proposed amendment would create a "classic moral hazard" through which CAT LLC's incentives to protect CAT Data would be diminished and would result in an underinvestment in cyber security.[18] Lewis further contends that Industry Members do not have access to CAT LLC's cyber security and lack the ability to verify if CAT LLC implements any suggestions from Industry Members.[19] Comment letters restate Lewis's claims, almost verbatim.[20]

1. Summary of CRA's Original Analysis as Applied to Lewis Report

At the outset, we note that neither Lewis nor the commenters appear to disagree with CRA's discussion of the economic literature regarding regulation and litigation.

By way of a brief recap, the CRA White Paper discussed the fundamentals of the choice between regulation and litigation (Section III.A). It investigated the economic determinants of the relative attractiveness of regulation or litigation to control risk as well as the conditions under which the joint use of each tool can be welfare enhancing (Section III.B). It presented the special considerations arising out of the CAT's situation (Section III.C). It applied the regulation and litigation approaches to a potential cyber breach at the CAT specifically by referencing the alignment of incentives and the additional costs that adding litigation by Industry Members would entail (Section III.D, especially III.D.2 and III.D.3). The CRA White Paper investigated the circumstances when litigation can have a meaningful role in aligning incentives and mitigating risk (see Section III.A), but then discussed the circumstances at the CAT that are not

[18] Lewis Report ¶¶ 12-13.

[19] "Industry Members do not have access to the details of CAT LLC's cyber security. . . Moreover, even if Industry Members could make suggestions that receive consideration, they would have no control or oversight on the implementation of these proposals or even a way to verify if the suggested changes have been made." Lewis Report ¶ 14.

[20] SIFMA, pp. 4 and 8; Letter from Thomas M. Merritt, Deputy General Counsel, Virtu Financial to Vanessa Countryman, Secretary, SEC, January 27, 2021, pp. 2-3, hereafter "Virtu"; Raymond James, p. 2; Citigroup, p. 2.

congruent with that literature. Lewis and the comment letters were generally silent on these issues.

Not only do Lewis and the commenters largely fail to engage with CRA's discussion of the economics of the regulation-litigation analysis, they also mischaracterize CRA's analysis and conclusions. Lewis states, for example, "The CRA Report also argues that there are no benefits to allowing Industry Members to sue CAT LLC, stating that 'adding the threat of litigation would do nothing to further internalize into the CAT's decision making the possible losses suffered by the Industry Members.'... This is another reason against the use of regulation as the only incentive."[21]

The crux of CRA's conclusion is not that there are no benefits to adding a threat of litigation; but rather, that the inconsequential and speculative benefits of adding that threat on top of the existing regulatory regime do not exceed the likely substantial costs. Further, neither Lewis nor any other commenter explains why the SEC's regulatory regime, combined with the overall regulatory structure that has been put in place within the context and circumstances for CAT, is insufficient to align the incentives of all relevant parties (not just those of the Industry Members) for cyber security at the CAT.

An important element of that context is the governance system that provides Industry Members unique access and ability to influence the CAT's cyber program. This governance mechanism is an appropriate response given CAT LLC's cost-only business model that currently provides no mechanism to establish safety reserves that might allow it to build a cash reserve to pre-fund catastrophic losses from a cyber breach. As a result, CAT LLC is not currently able to cover a substantial cyber loss (particularly if those costs would exceed available insurance coverage). As noted in the CRA White Paper, the academic literature discusses the limitations of litigation to provide incentives for managers to take precautions when they believe there is a possibility they will be unable to pay fully the amount of the loss should it occur. The literature notes that in these circumstances, regulatory systems are preferable to encourage the responsible party to invest in safety. Regulation is one way to compel the first party to internalize expected social costs of losses suffered by third parties, incorporating those third-party costs into the first-party's decision making. Providing third parties access to information about the operations of the first party and the ability to influence the behavior of the risk-taking of the first party is another way to compel the first party to internalize the expected social costs of losses.

Absent the ability to litigate against CAT LLC, FINRA CAT, or the Participants for damages, Industry Members have incentives to deploy resources to exercise their governance rights on the Advisory Committee, monitor the cyber program at the CAT, and lobby for changes they deem in their interests. Removing the limitation of liability provisions may have the unintended consequence of reducing Industry Members' incentives to undertake these costly monitoring activities in favor of relying upon the threat of litigation.

To understand one aspect of the unique regulatory circumstances facing CAT LLC, we call attention to the Advisory Committee and the role of Industry Members on it. Critically, as the CAT NMS Plan provides, "[m]embers of the Advisory Committee shall receive the same information concerning the operation of the Central Repository as the Operating Committee;

[21] Lewis Report ¶ 22.

provided, however, that the Operating Committee may withhold information it reasonably determines requires confidential treatment."[22] The SEC added this provision to the CAT NMS Plan in response to comments.[23] In approving that amendment, the Commission noted that it "believes it is important for the Advisory Committee to fulfill its role that its members receive full information on Plan operations (other than confidential information) and that it is therefore appropriate to amend Section 4.13(e) of the Plan accordingly."[24] It is clear that outside parties, especially Industry Members, have significant insight and influence regarding the cyber security of the CAT (a fact that Lewis does not acknowledge).[25] The SEC seems to agree.[26]

Another notable omission in Lewis's examination of the CAT's cyber security is the role of Amazon Web Services ("AWS") as the CAT's primary technology provider. AWS is the "most flexible and secure cloud computing environment available today. [Its] core infrastructure is built to satisfy the security requirements for the military, global banks, and other high-sensitivity organizations."[27] Many types of CAT breaches, particularly but not only from an external source, would have to surmount AWS's security perimeter and the CAT's cyber security (including the SEC's regulatorily mandated measures). Critically, a CAT breach would harm AWS's reputation as a cloud computing environment supplier. This reputational consideration would also apply to the CAT's other cyber security vendors and consultants. There is no recognition of this *ex-ante* incentive alignment mechanism anywhere in either Lewis's report or any comment letter.

2. Lewis's Discussion of Moral Hazard

Lewis also claims that the Proposed Amendment "would result in a classic example of moral hazard, where CAT LLC's incentives to invest in data security would be diminished since Industry Members, rather than CAT LLC, would bear the potential litigation costs of a breach or misuse of CAT Data."[28] The Citadel comment letter also asserts a version of this claim.[29]

Contrary to these assertions, the Proposed Amendment is not a "classic example" of a moral hazard. A moral hazard occurs when a party can enter into a contract with an agent and the agent can subsequently change its behavior in a manner that provides it private benefits. A moral hazard exists when the principal party has limited ability to learn about or monitor the behavior of the party with whom it has contracted with, or it lacks tools to address a change in the agent's behavior. Critically, moral hazards require incomplete information such that the

---

22 Securities and Exchange Commission, *Order Approving CAT Exhibit A*, "Limited Liability Company Agreement of CAT NMS, LLC, a Delaware Limited Liability Company," hereafter "*CAT LLC Agreement,*" Section 4.13(e).

23 SEC, *Order Approving CAT*, Section IV.B.2, p. 155.

24 SEC, *Order Approving CAT*, Section IV.B.2, p. 156.

25 SEC, *Order Approving CAT*, Section IV.B.1, pp. 139-140.

26 SEC, *Order Approving CAT*, Section IV.B.2, p. 155 ("the interests of the industry and other stakeholders have been represented through the DAG [and] the public comment process. . .").

27 Amazon Web Services website, "Cloud computing with AWS, Most secure" at https://aws.amazon.com/what-is-aws/?sc_icampaign=aware_what_is_aws&sc_icontent=awssm-evergreen-prospects&sc_iplace=hero&trk=ha_awssm-evergreen-prospects&sc_ichannel=ha, visited March 2021.

28 Lewis Report ¶ 12.

29 Citadel, pp. 7-8.

agent's change in behavior is not understood by both parties.[30] This is not the situation here. In this case, Industry Members have meaningful ability to both monitor and influence outcomes at the CAT, particularly in relation to cyber security.

Relatedly, Citadel contests the claim that the Advisory Committee has both visibility and influence over cyber security at the CAT.[31] Citadel's claim, however, cannot be reconciled with the regulatory regime and the documented history of cyber security changes mandated by the SEC. Indeed, the SIFMA letter implicitly acknowledged the industry's ability to influence CAT's cyber security by stating that "[t]he 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."[32]

3. The Internalization of Costs and the Public Interest

Lewis claims "[t]he costs not being internalized by CAT LLC are the litigation costs related to breaches of the CAT Data that would instead be borne by Industry Members under the Proposed Amendment."[33] Lewis then states that:

> *[T]he analysis in the CRA Report ignores risks and costs associated with customers of Industry Members potentially bringing suit against Industry Members if their data is compromised … If the costs related to such litigation were also considered in the CRA Report's economic analysis, it would show that requiring the parties that have access to and are responsible for protecting the data to bear these costs leads to better incentive alignment*.[34]

Concerns that the costs of a cyber breach at the CAT are being sidestepped by the Participants and imposed upon Industry Members are not supported by a considered understanding of the system as a whole. First, as already explained above, the limitation of liability provisions apply only to signatories to the CAT Reporter Agreements (and to CAT LLC and certain representatives defined in the Reporter Agreements, including the Participants). The SEC is not a signatory. Second, as a result of their roles on the Advisory Committee, Industry Members have access to information about the performance of the CAT's cyber program and the ability to influence changes. Under this system, Industry Members have incentives, and the ability, to share with CAT LLC information about their expected loss costs due to different cyber breach scenarios and the ability to seek changes. Additionally, Industry Members have the ability to directly lobby the SEC to mandate changes should they believe that the Participants are not sufficiently taking their position into account.

Lewis opines that CAT LLC should be incentivized to invest in security in a manner that considers all costs of operating the CAT (including indirect costs such as litigation incurred by

---

30 Steven Nickolas, "Understanding the Difference Between Moral Hazard and Adverse Selection," *Investopedia*, September 16, 2020, at https://www.investopedia.com/ask/answers/042415/what-difference-between-moral-hazard-and-adverse-selection.asp, accessed March 2021.

31 Citadel, p. 9.

32 SIFMA, p. 6; see also Citadel, p. 2 ("[T]he Commission in August 2020 proposed enhancements to the security of CAT data, which included proposed amendments to the CAT NMS Plan designed to improve the security of CAT data that is extracted from the CAT by a Participant.").

33 Lewis Report ¶ 15.

34 Lewis Report ¶¶ 20, 21.

parties other than CAT LLC, the Participants, and FINRA CAT) and that the most effective method of creating those incentives is for CAT LLC to be liable for damages.[35] Lewis claims that while CAT LLC has some incentive to invest in cyber security, "the marginal costs and benefits faced by CAT LLC to invest further in data security are no longer the same as Industry Members under the Proposed Amendment since Industry Members may be sued by their customers should the data be compromised, but Industry Members cannot sue CAT LLC to recover any related costs."[36] Two commenters reiterate this point. [37]

These excerpts from the Lewis Report and comment letters are revealing because they suggest that the industry's concern is not for the investing public or the fair and efficient operations of the U.S. equity and options markets, but instead the financial condition of Industry Members themselves. Lewis has not proven, nor can he prove, that the interests of the Industry Members in cyber security at the CAT coincide with those of the investing public or the equity and options markets. But the public's interest in the CAT and cyber security at the CAT are not subsumed within the interests of the Industry Members as Lewis and the Industry Member comment letter writers presume.

By contrast, CRA's analysis focused on enhancing social welfare and investor protection. As discussed in the CRA White Paper, the limitation of liability provisions further those important goals. As the CRA White Paper demonstrates, the SEC is the best protector of the public's interest given its unique ability to regulate the CAT. In addition, the SEC has the expertise and the mandate to balance every relevant interest, not just the pecuniary interests of Industry Members.

4. *Ex-Ante* Regulation Plus *Ex-Post* Litigation for CAT Cyber Security

Lewis disagrees with CRA's conclusion that social welfare would decrease if Industry Members gained *ex-post* litigation rights to sue for damages in the event of a cyber breach of the CAT, instead arguing that: (1) CRA ignores the risks and costs of potential lawsuits filed against Industry Members by their clients following a cyber breach at CAT; (2) Industry Members will be forced to inefficiently purchase additional liability insurance to protect themselves from lawsuits filed by their clients following a breach; and (3) affording Industry Members the right to sue for damages will uniquely increase CAT's willingness to invest in improvements in the cyber security program as new technologies emerge.

At the outset, we note that Lewis and comment authors misread the CRA analysis as if it assumed that the Proposed Amendment requires the SEC to choose between regulation and litigation in a vacuum. But in the description of CRA's assignment, the CRA White Paper explicitly acknowledged that:

> *In reviewing CAT LLC's proposed plan amendment for a limitation of liability, the Commission is faced with the choice of* ***whether to supplement the cyber regulatory regime that the Commission has already imposed*** *by affording Industry Members the ability to bring private litigation against CAT LLC and the Participants. Based on our application of*

[35] Lewis Report ¶ 16.
[36] Lewis Report ¶ 17.
[37] SIFMA, p. 9, emphasis added; Raymond James, pp. 1-2.

> *the economic literature, we conclude that regulation alone is preferable to regulation plus litigation.*[38]

CRA's principal conclusion is that given the extensive cyber security regulatory regime already mandated by the SEC (among other factors), the addition of litigation from Industry Members would not improve the alignment of incentives for cyber security at the CAT. Neither the Lewis Report nor the comment letters provide any basis to undermine that conclusion.

Lewis claims that CRA's analysis ignores the costs associated with lawsuits brought against Industry Members, and that if such costs were considered, the analysis would show that the party who controls the data should bear liability.[39] SIFMA similarly suggests that the CRA analyses ignore potential lawsuits against Industry Members brought by clients.[40] As noted previously, Lewis and SIFMA assume, without support, that Industry Members will face litigation risk from their customers due to a cyber breach at the CAT. We discussed previously that regulatorily-mandated provisions and governance mechanisms provide Industry Members significant *ex-ante* visibility into and influence over the cyber security program at the CAT. Critically, these same mechanisms also enable Industry Members to share with the Participants and the SEC information about their expected losses in the event of a cyberbreach such that the regulators can evaluate whether and how to address these events (including, potentially, through the use of limitations on liability that Industry Members impose on their own customers).

Lewis subsequently argues that Industry Members will be forced to inefficiently purchase additional liability insurance.[41] A number of potential parties could incur losses following a cyber breach at the CAT including: the Participants, individual investors, institutional investors, technology suppliers to CAT LLC, and Industry Members themselves, among others. Industry Members certainly have first party exposure to the CAT as they may experience losses due to a data breach. Purchasing cyber liability insurance to protect against potential first-party losses might be part of a reasonable and sound approach to managing this first-party risk exposure.

Lewis's conclusion that Industry Members would face third-party damage claims for a CAT Data breach rests on a continuation of his unsupported premise that Industry Members will be liable to their customers in the event of a CAT cyber breach. This error undermines the conclusions that Lewis draws regarding the purchase of insurance against such a third-party risk.

Lewis and Citadel both suggest that the regulatory mandates will eventually become insufficient as underlying changes in technology are inherently too fast for the SEC to keep up the regulatory apparatus up-to-date. Thus, they argue that litigation in addition to regulation is necessary to give CAT LLC an added incentive to stay ahead of the SEC's regulations as technology changes.

There are several weaknesses with this line of reasoning. First, Lewis and Citadel ignore that the Participants and FINRA CAT are required to monitor CAT's cyber security and promptly address any vulnerabilities under the terms of the SEC's regulation.[42] Second, as discussed previously, CAT LLC's governance and operating mechanisms gives Industry

---

38 CRA White Paper p. 33.
39 Lewis Report ¶ 20.
40 SIFMA, p. 9.
41 Lewis Report ¶ 21.
42 *CAT LLC Agreement,* Section 6.5(f).

Members unique capabilities to educate and influence both CAT LLC and the SEC, including regarding potential cyber security enhancements. Third, Lewis and Citadel fail to consider that the SEC has unique access to some of our nation's most highly sophisticated cyber security and cyber warfare assets, including the National Security Agency, the Department of Homeland Security, and the Cybersecurity & Infrastructure Security Agency, and thus is able to employ the most up-to-date technology. Fourth, Lewis and Citadel discount the reputational incentives of the CAT's technology suppliers (AWS, etc.) to maintain the CAT's cyber defenses. Fifth, it is not clear that providing Industry Members a right to recover substantial damages from CAT LLC or the Participants will further internalize CAT LLC's, FINRA CAT's, or the Participants' expected loss costs into the decision-making of CAT managers given the governance mechanisms that already exist at CAT and, if litigation weakens Industry Members' incentives to provide feedback to the Participants, the ability to sue for damages may have the unintended consequence of increasing CAT cyber risk. Sixth, assuming for the sake of argument that the SEC is unable to keep pace with changing technology, the Participants still potentially face litigation risk including from SEC enforcement actions.

Finally, Lewis and commenters offer an optimistic view of the efficacy of litigation to improve the cyber security in the context of the CAT. Litigation typically proceeds slowly, and it is far from clear that litigation would result in a resolution faster than regulation. In addition, no matter how uncertain regulation is, we are aware of no evidence that a litigation result is preferred or even more "certain" on an *ex-ante* basis. We do not believe that substituting the judgement of lay jurors or judges is superior to that of the experts in cyber security and financial markets available to the SEC and CAT LLC, especially in this circumstance when the SEC oversight of CAT is particular to CAT so its rules and regulations can be written with precision. Additionally, Section III.D.3 of the CRA White Paper addresses the incremental costs of litigation in the context of CAT cyber security. The CRA analysis demonstrates that the costs of litigation far outweigh the benefits in the context of the CAT, and Lewis provides no reason to doubt that conclusion.

Citadel and Lewis both suggest it could be more welfare enhancing to provide Industry Members with the right to litigate against CAT LLC, the Participants, and FINRA CAT for damages in addition to the SEC's regulatory regime.[43] The relevant academic literature (which Lewis does not discuss) does not support Lewis's or Citadel's arguments. Harvard economist Professor Steven Shavell and University of Cologne economist Professor Patrick Schmitz, for example, consider settings where the underlying regulated risky behavior is being carried out by multiple firms in the economy.[44] In those instances, a minimal regulatory regime that relies on courts to tailor the general negligence standard to the specific circumstances and conduct of each firm is the optimal outcome. But, as discussed in the CRA White Paper, that is not the case here, because the Commission can (and does) target its cyber security regulation of the CAT specifically to the CAT.

Research by Kolstad, Ulen and Johnson published in the *American Economic Review*, the flagship scholarly journal published by the American Economic Association, analyzes cases

---

43 Citadel, pp. 9-10.

44 Steven Shavell, "Liability for Harm Versus Regulation of Safety," *The Journal of Legal Studies*, Vol. 13, No.2 (June 1984), pp. 357-374; Schmitz, Patrick W., "On the Joint Use of Liability and Safety Regulation," *International Review of Law and Economics,* Vol. 20, No. 3 (September 2000), pp. 371-382.

where courts apply the negligence standard to accidents, and demonstrates that adding *ex-ante* regulation (to existing litigation) is efficiency enhancing to ensure a minimal level of investment in safety by the firm engaged in the risky activity.[45] But their research does not apply here because the CAT is a highly regulated entity, and the question under consideration is whether it is efficiency enhancing to add *ex-post* litigation. That research also does not envision a circumstance, such as the one that applies to the CAT, where those who might suffer losses (i.e., Industry Members) would have input regarding the risk management program of the firm.

5. Lewis on Existing Limitation of Liability Provisions in the Securities Industry

Lewis contends that existing limitation of liability provisions that apply to OATS provide an inappropriate comparison to the proposed limitation of liability in the CAT Reporter Agreements for three reasons: (1) the CAT Data is "far more comprehensive" and contains "much more valuable information" than that covered previously, (2) "the CAT System was designed with regular access in mind" and the "likely more frequent and broader use of this data exposes it to a great risk." and (3) the prior limitation of liability provisions were signed "more than two decades ago."[46]

It is undeniable that the trading data downloaded to the CAT is more comprehensive than trading data collected by OATS, though Lewis and others fail to explain why this is a differentiating factor for the limitation of liability. CAT Data, for example, requires more granular reporting of trading activity. That CAT Data will experience "more frequent and broader use" is also most likely to be true. But Lewis fails to explain why the existence of more comprehensive data could justify changing the traditional industry standard allocation of liability between the Participants and Industry Members.

Lewis also does not reference that CAT LLC is collecting this data under a mandate from the SEC in response to changing technology and market structure. The SEC and others have recognized that modern financial markets need more comprehensive trading data than has existed in the past, and that regulators must access that data more often. Commensurate with recognizing this need, the SEC and all other interested parties also recognize the risk of a cyber breach at the CAT and the SEC has mandated extensive cyber protections. Lewis provides no evidence nor meaningful analysis as support for his contention that, when viewed in its entirety, the investing public would benefit from the ability of Industry Members to litigate for damages on top of the existing regulatory regime. The fact that a limitation of liability provision for another regulatory reporting facility (OATS) was signed "more than two decades ago" is not a compelling economic argument in support of the proposition that the proposed limitation of liability provisions should not be used in connection with CAT reporting—especially considering that it is industry standard for Industry Members, the Participants, and NMS Plans to have limitation of liability provisions.

---

[45] Kolstad, Charles D., Thomas S. Ulen, and Gary V. Johnson, "*Ex Post* Liability for Harm vs. *Ex Ante* Safety Regulation: Substitutes or Complements?" *The American Economic Review* Vol. 80, No. 4 (Sep. 1990), pp. 888-901.

[46] Lewis Report ¶¶ 24-26

B. Optimal Insurance Coverage to Reimburse Investors in the Event of a Cyber Breach

Lewis asserts that the Proposed Amendment would lead to CAT LLC purchasing a suboptimal amount of insurance and that "investors would be better off if insurance was purchased by CAT LLC, which is responsible for safeguarding the data, as opposed to Industry Members which face higher premiums from insurers because they do not have access to the CAT System or control of its security measures."[47] SIFMA and Citadel echo Lewis's position.[48] This position is unpersuasive because we have been informed that CAT LLC has purchased the maximum amount of insurance that the market would viably offer at the time, and Lewis's assertions regarding insurance for Industry Members is unsupported by the evidence.

1. Lewis on Insurance Premiums and Insurers' Ability to Monitor

Lewis asserts that"[i]t is important to note that if a cyber-breach occurred, it is likely to be a single event that affects all Industry Members simultaneously."[49] CRA's scenario analysis does not support that proposition (and Lewis did not conduct his own scenario analysis).[50] Lewis also does not explain why a single event simultaneously affecting all Industry Members instead of multiple events affecting subsets of Industry Members makes a difference.[51] Lewis seems to imply that a single event simultaneously affecting all Industry Members might weaken the insurance mechanism when he writes, "from the standpoint of an insurer … this is unlike the typical situation where the pooling of risk can reduce the volatility around claims."[52] Lewis presents a narrow view of how risk is diversified across the insurance industry. Although he is correct to note that correlated risks limit the benefits of diversification in an insurance pool, insurers are able to spread correlated risks through reinsurance contracts across the global insurance industry ultimately bringing the benefits of diversification to all who are insured. Hurricane risk in Florida is certainly highly correlated in the book of business for a Florida insurance company, yet it can be successfully underwritten when it is reinsured and diversified with Japanese tsunami risk, or some other uncorrelated risk, with the help of a global reinsurer.

As was discussed in the CRA White Paper, purchasing insurance is a sound economic practice for CAT LLC for several reasons, including the pooling of risk as a way to reduce expected costs (despite Lewis' assertion discussed above). The CRA White Paper also highlights that purchasing insurance extends the assets available to pay losses in the event of a cyber breach and therefore provides greater incentives for CAT managers to take precautions. Additionally, as discussed in the CRA White Paper, insurance provides compensation to injured parties, and, as Lewis recognizes in Paragraph 34 of his report, "Monitoring and engagement by insurers may also lead to certain suggestions or requirements that can both lower the cost of insurance as well as improve the overall security of CAT LLC."[53]

---

47 Lewis Report ¶ 30.
48 SIFMA, p. 8; Citadel, pp. 8-9.
49 Lewis Report ¶ 31.
50 The scenario analyses in the CRA White Paper include examples where only one Industry Member could be affected, such as bad actors seeking to reverse engineer a trading algorithm (Scenario 3, pp. 24-26).
51 Lewis Report ¶ 31.
52 Lewis Report ¶ 31.
53 Lewis Report ¶ 34.

Lewis proceeds in Paragraph 34 to make the erroneous claim that if Industry Members purchase their own cyber insurance, not only would their insurers be unable to monitor CAT LLC, but even if they did have suggestions for how to strengthen the cyber program at CAT, "Industry Members have no ability to force CAT LLC to comply and adopt the suggested security protocols."[54] As noted above, Industry Members participate in the Advisory Committee and can present their concerns to the SEC, which can decide whether to add proposed cyber security measures. In addition, the SEC and, especially, the CAT's security providers and consultants also have the ability and motivation to monitor the CAT's cyber security protections.

2. Lewis on CAT LLC Obtaining Additional Insurance

Lewis critiques CRA's discussion of CAT LLC's cyber insurance program on the grounds that CRA does not offer details regarding the coverage that CAT LLC has in place. [55] Commenters reiterate Lewis's critique.[56] There are three principal responses to Lewis and the commenters.

First, one of the fundamental principles of cyber security is to avoid providing hackers with information about security protocols or potential rewards for a successful breach. Disclosing the information Lewis and SIFMA requested in a public document (like the Proposed Amendment) would help hackers better understand the reward for a successful breach.[57]

Second, Lewis again fails to consider Industry Members' role with respect to CAT's cyber security. As participants in the Advisory Committee, Industry Members have the ability to raise their concerns regarding CAT LLC's insurance to the Participants and to the SEC, and to propose specific adjustments for the Commission's consideration.

Third, because the market for cyber liability insurance is relatively new and the insurance industry's ability to supply coverage is still developing, it is possible that additional coverage will become available to CAT LLC in the future. More mature insurance markets are able to expand supply while continuing to charge close to actuarially fair premiums regardless of the amount of consumer demand. The amount of cyber liability insurance the market is willing to provide, on the other hand, is finite as prices for insurance are characterized by increasing price margins for increasing amounts of coverage. For comparison, insurance carriers wrote $2.3 billion direct premiums written for package and standalone cyber products in 2019[58] versus $80.5 billion Other Liability insurance coverages.[59] Lewis's contention that all potential liability

---

54 Lewis Report ¶ 34.

55 Lewis Report ¶ 36.

56 SIFMA, p. 8; Citadel, pp. 8-9.

57 See, for example, Erin Ayers, "This week in cyber risk: Cyber insureds are 'the tastiest morsels' for ransomware actors," *Advisen Cyber Front Page News*, March 19, 2021, at https://www.advisen.com/tools/fpnproc/news_detail3.php?list_id=35&email=mmeyer@crai.com&tpl=news_detail3.tpl&dp=P&ad_scale=1&rid=392891790&adp=P&hkg=rGjYsTVgZt, accessed March 2021.

58 Aon, "US Cyber Market Update: 2019 US Cyber Insurance Profits and Performance," (June 2020), p. 3.

59 National Association of Insurance Commissioners, "The Property/Casualty Market Share Report," (March 30, 2020) accessed March 21, 2021 at https://www.naic.org/documents/web_market_share_property_casualty.pdf.

insurance be supplied by the CAT alone and that this will necessarily be more cost efficient is not correct given the current state of the cyber insurance marketplace.[60]

V. Response to Two Issues Raised in Public Comment Letters

There are two issues raised in comment letters, but not addressed by Lewis, that merit a response from the perspective of economic analysis. First, certain commenters argue that any limitation of liability that the Commission approves should contain various exclusions. Second, commenters incorrectly claim that CRA's scenario analysis is incomplete because it did not address threats from bad actors within FINRA CAT or the Participants.

A. Response to Commenters' Proposed Exclusions

SIFMA claims that "the Proposal would effectively extinguish the liability of CAT LLC and the SROs even in instances of gross negligence or intentional misconduct [and that] "[a]t the very least, 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."[61] Citadel opined that "[t]he Commission should reject the Proposal because the Provisions would insulate the Participants and their representatives when engaging in misconduct outside their regulatory responsibilities."[62]

Insight from economic theory suggests that Industry Members' proposed exclusions are unwarranted. First, the comment letters do not acknowledge that instances of gross negligence, willful misconduct, bad faith, criminal acts, and the use of CAT Data outside of the regulatory context are already subject to enforcement action by the SEC. Second, adding commenters' proposed exclusions to the limitation of liability provisions would potentially generate substantial litigation. Competent litigators will likely try to satisfy pleading standards even when the facts may be inconsistent with such claims.

In that regard, the lessons from tort reform illustrate the potential negative impact on social welfare of allowing Industry Members to sue for gross negligence, recklessness, or willful misconduct. Following the insurance availability crisis in the 1980s, states enacted a number of tort reforms among which included caps on punitive damage awards and that raised the standards to state a claim for gross negligence. Economists who have investigated the question of how the tort reforms impacted accident rates found support for the hypothesis that enacting the reforms led to lower accident rates or accident severity generally. For example, Paul Rubin and Joanna Shepherd, in research published in the leading peer-reviewed law and economics scholarly journal, investigate the relationship between tort reform and accidental death rates in the United States using data from 1981 through 2002. They find most reforms, including caps on punitive damages, are associated with fewer accidental deaths.[63]

---

60 For a discussion of the challenges to the further development of the cyber insurance market, see Chapter 4 in OECD, *Enhancing the Role of Insurance in Cyber Risk Management*, (2017), OECD Publishing, Paris.

61 SIFMA, pp. 5 and 7-8.

62 Citadel, p. 3.

63 Paul H. Rubin and Joanna M. Shepherd, "Tort Reform and Accidental Deaths," *Journal of Law and Economics* Vol. 50 No. 2 (May 2007), pp. 221-238.

There are at least three reasons to believe that enacting tort reforms (including imposing obstacles to stating claims for gross negligence) might decrease loss producing behavior. First, the reform affects the incentives of potentially injured parties. Knowing they will receive less compensation when there is a loss may incentivize potentially injured parties to make greater investments in precautions themselves, which may decrease frequency and severity of accidents. In the present case, limiting Industry Members' ability to recover damages provides them greater incentives to provide feedback to CAT's management by exercising their rights to participate on the Advisory Committee.

Second, the reduced expected liability costs may free up resources that allow parties to allocate more resources to risk reducing products or services. In this case, reducing expected liability costs may provide additional resources to further enhance the CAT's cyber security program or to purchase cyber liability insurance as it becomes available. Investment in cyber security beyond an optimal level reduces the resources available for competing CAT priorities, such as investments in infrastructure to make the CAT faster and easier to use. The Commission has a unique ability to balance these competing interests. Courts, in contrast, lack the information and broader perspective necessary to account for all relevant interests.

Third, the reduced variability on the size of damage payments makes liability costs more predictable, which reduces the amount of capital an insurer needs to allocate to the line of insurance in order to guaranty a prescribed level of solvency for the insurance carrier. Since capital is costly, decreasing the amount of capital necessary for the insurer to maintain a particular level of creditworthiness will reduce the cost of insurance.[64] At a minimum, reducing insurance costs will increase the demand for insurance and it may also increase the supply of insurance available in the marketplace.

B. Data Breaches Originating from within CAT

The second argument made in the comment letters that does not appear in the Lewis Report is the assertion that the CRA White Paper focused only on breaches by external factors and failed to address misuse of CAT Data by CAT personnel and other potential internal sources.[65]

That characterization of the CRA cyber risk analysis is simply incorrect. The CRA risk assessment is not "focused almost exclusively" on external malicious actors. Rather, the CRA risk assessment is agnostic with respect to the motivations or employment of potential perpetrators of a cyber breach. It posits a number of illustrative adverse cyber events and evaluates them along several dimensions. Whether a perpetrator is external or internal makes no difference to the scenario analysis. Notably, the Citadel comment letter raises this purported "flaw" but does not explain how (or even if) it undermines the regulatory-litigation tradeoff or the effect of the proposed limitation of liability provisions.[66]

Finally, we believe that commenters' purported concerns about the threat of "internal" breaches are exaggerated. All Participant users of CAT Data are subject to comparable cyber

---

64 Daniel Bauer, Richard D. Phillips, and George Zanjani, "Financial Pricing of Insurance," (2013) in *Handbook of Insurance Economics 2nd Edition,* edit by Georges Dionne, Boston: Kluwer Academic Publishers.

65 SIFMA, p. 9; Citadel, pp. 2, 6; Virtu, p. 5; see also Raymond James, p. 2.

66 Citadel, p. 6.

security procedures and protocols whether the data remains on the CAT system or is downloaded.[67] In addition, only trading data, not customer data, can be downloaded in bulk.[68]

VI. Conclusion

Following a review of the economic issues raised by Lewis and commenters, we maintain our principal conclusions, including that the regulatory approach alone leads to the socially desirable level of investment in cyber security and protection of CAT Data. Allowing Industry Members to litigate for damages against CAT LLC, the Participants, and FINRA CAT in the event of a cyber breach would result in increased costs overall without any meaningful benefit to the CAT's cyber security. We thus reiterate our primary conclusion: the limitation of liability is well supported by applicable economic principles, especially considering the framework of the SEC's mission and its mandates regarding the CAT.

Lewis and certain commenters generally fail to appreciate the substantial incentives created by the SEC's overall approach to cyber risk management at the CAT. Indeed, the Commission has enacted an extensive regulatory regime mandating specific cyber standards, policies, procedures, systems, and controls that CAT LLC and the Plan Processor must implement. This regulatory approach was developed with extensive feedback from Industry Members and is subject to ongoing review and modification through a public review and comment process. The Participants' compliance with the requirements of this regulatory regime can be policed by the SEC's Enforcement Division. Lewis and other commenters fail to explain why the incentives created by the SEC's regulatory oversight (in conjunction with other sources of incentives including reputational risk, oversight from AWS and diligence by insurance carriers) are insufficient to ensure optimal investments in cyber security.

Relatedly, Lewis and commenters fail to consider the consequences of the CAT's financing principles that reduce the effectiveness of litigation to provide incentives to internalize Industry Member concerns and the corresponding meaningful input that Industry Members have regarding the CAT's cyber security through their participation in the Advisory Committee and the ability to directly petition the Commission for rulemaking. Industry Members' role on the Advisory Committee provides them with the ability to advocate for their interests regarding CAT's cyber security. The irony of the position of certain Industry Members' is that not including limitation of liability provisions in the CAT Reporter Agreements attenuates Industry Members' incentives to contribute their feedback on cyber security to CAT LLC. If Industry Members can litigate against CAT LLC for damages, they have less reason to diligently monitor the CAT and raise any suggestions to the Participants and the SEC. So, the opposition of the Industry Members is itself an indication that the public interest is better served by adopting the Proposed Amendment.

We also find no support, from the perspective of economic analysis, for the proposals from SIFMA and certain Industry Members to exclude certain categories of conduct (e.g., gross negligence, bad faith) from the limitation of liability. In the analogous context of tort reform,

---

67 SEC, *Order Approving CAT,* Section IV.D.6, p. 253.

68 Letter from Michael Simon, CAT NMS Plan Operating Committee Chair to Vanessa Countryman, Secretary, SEC, April 1, 2021, p. 11, Footnote 42, ("PII such as SSN and TIN will not be made available in the general query tools, reports, or bulk data extraction.").

evidence exists in the literature that demonstrates decreasing the availability of claims for gross negligence did not increase loss-producing behavior. In the context of the CAT, we would not expect disclaiming liability for gross negligence, recklessness, and intentional misconduct to increase the likelihood of breaches. We would, however, expect including those carveouts in the limitation of liability to substantially increase CAT LLC's costs (which will ultimately be passed along to all market participants) with no corresponding benefit.

Finally, we have reviewed the arguments from Lewis and commenters regarding CAT's insurance and do not find them persuasive. We know of no valid basis to question CAT LLC's assertion that it has purchased the maximum amount of viable insurance coverage.