April 1, 2021

VIA EMAIL

Vanessa Countryman
Secretary
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Re: File No. 4-698: Notice of Filing of Amendment to the National Market System Plan Governing the Consolidated Audit Trail

Dear Ms. Countryman:

On January 6, 2021, the Securities and Exchange Commission ("SEC" or "Commission") published a notice of filing of amendment to the National Market System Plan Governing the Consolidated Audit Trail (the "CAT NMS Plan" or "Plan")[1] pursuant to Rule 608 of Regulation NMS ("Rule 608")[2] under the Securities Exchange Act of 1934 (the "Exchange Act").[3] As described more fully in the proposed amendment (the "Proposed Amendment"), the Participants[4] seek to revise the Consolidated Audit Trail Reporter Agreement (the "Reporter Agreement") and the Consolidated Audit Trail Reporting Agent Agreement (the "Reporting Agent Agreement") to insert the limitation of liability provisions (the "Limitation of Liability Provisions") contained in Appendix A to the Proposed Amendment. Those provisions would address the liability of CAT LLC, the Participants, and FINRA CAT in the event of a CAT Data breach.

The SEC received eleven comment letters in response to the Proposed Amendment. The Participants submit this correspondence to respond to the issues raised in those comment letters. In general, commenters focused on: 1) industry standards and public policy concerns regarding the allocation of liability between the Participants and Industry Members, 2) the cybersecurity of CAT

---

[1] The CAT NMS Plan is a national market system plan approved by the Commission pursuant to Section 11A of the Exchange Act and the rules and regulations thereunder. *See* SEC, Joint Industry Plan; Order Approving the National Market System Plan Governing the Consolidated Audit Trail, Release No. 34-79318; File No. 4-698 (Nov. 15, 2016), hereinafter "SEC, Order Approving CAT NMS Plan," available at https://www.sec.gov/rules/sro/nms/2016/34-79318.pdf, 81 Fed. Reg. 84696 (Nov. 23, 2016), available at https://www.govinfo.gov/content/pkg/FR-2016-11-23/pdf/2016-27919.pdf. The full text of the CAT NMS Plan as amended is available at https://www.catnmsplan.com/sites/default/files/2020-02/CAT-2.0-Consolidated-Audit-Trail-LLC%20Plan-Executed_%28175745081%29_%281%29.pdf.

[2] 17 C.F.R. § 242.608, available at https://www.govinfo.gov/content/pkg/CFR-2006-title17-vol3/pdf/CFR-2006-title17-vol3-sec242-608.pdf.

[3] Unless otherwise defined herein, capitalized terms used herein are defined as set forth in the CAT NMS Plan.

[4] The twenty-five Participants of the CAT NMS Plan are: BOX Exchange LLC; Cboe BYX Exchange, Inc., Cboe BZX Exchange, Inc., Cboe EDGA Exchange, Inc., Cboe EDGX Exchange, Inc., Cboe C2 Exchange, Inc. and Cboe Exchange, Inc., Financial Industry Regulatory Authority, Inc., Investors Exchange LLC, Long-Term Stock Exchange, Inc., MEMX LLC, Miami International Securities Exchange LLC, MIAX Emerald, LLC, MIAX PEARL, LLC, Nasdaq BX, Inc., Nasdaq GEMX, LLC, Nasdaq ISE, LLC, Nasdaq MRX, LLC, Nasdaq PHLX LLC, The NASDAQ Stock Market LLC; and New York Stock Exchange LLC, NYSE American LLC, NYSE Arca, Inc., NYSE Chicago, Inc., and NYSE National, Inc.

Data, 3) the regulatory nature of the CAT, and 4) the economic analysis conducted by Charles River Associates ("Charles River") filed with the Proposed Amendment. Additionally, the Securities Industry and Financial Markets Association ("SIFMA") submitted a report by Professor Craig M. Lewis responding to Charles River's conclusions. Finally, commenters made suggestions regarding potential methods to compensate Industry Members in the event of a CAT cyber breach.

Following a thorough review and consideration of the issues raised by commenters, the Participants maintain that the Proposed Amendment is consistent with the Exchange Act. At bottom, commenters who opposed the Proposed Amendment are asking that their primary regulators (including, in the opinion of an industry trade association, the Commission itself) bear any and all liability for hypothetical "black swan" cyber breaches. That extraordinary ask is simply without precedent.

None of the comments overcame the core premise of the Proposed Amendment—that the Participants are implementing a regulatory mandate in their regulatory capacities and should therefore receive the liability protections they are customarily afforded when implementing their regulatory responsibilities pursuant to the direction and oversight of the Commission. And no commenter offered a compelling rationale as to why the longstanding principles regarding allocation of liability between securities self-regulatory organizations ("SROs") and Industry Members—as memorialized in the Commission-approved rules of every securities exchange and in agreements for NMS facilities and regulatory reporting facilities—should not apply to CAT reporting.

Further, the comments overlook the Commission's comprehensive oversight of CAT operations, including with respect to cybersecurity. The Commission approved the CAT's robust cybersecurity framework when it approved the Plan, and the Commission continues to address these issues on an ongoing basis. In opposing the Limitation of Liability Provisions, commenters are, in essence, seeking the ability to second-guess the Commission's determinations in court.

The Participants respectfully request that the Commission approve the Proposed Amendment.

A. Background

Several commenters suggest that the Participants and Industry Members would be better served continuing negotiations to resolve the allocation of liability dispute—despite SIFMA's refusal to respond to numerous proposals by the Participants to revise the Limitation of Liability Provisions to address the industry's stated concerns. Commenters also mischaracterize the settlement of an administrative proceeding between SIFMA and the Participants as having resolved the question of whether the Limitation of Liability Provisions should be included in the Reporter Agreement (and the Reporting Agent Agreement). It did not. The Participants address both comments below.

1) Negotiations Between the Participants and Industry Members

With respect to the Participants and Industry Members continuing negotiations to resolve the allocation of liability disagreement, one commenter stated that rather than filing the Proposed

Amendment, "it may have been much more useful if all market participants had come together to discuss where the liability from a breach should fall."[5] Another commenter noted that the Participants and Industry Members had exchanged "extensive correspondence and communications" to address the proper allocation of liability in the event of a CAT Data breach.[6]

The Participants generally agree that the parties previously engaged in meaningful discussions regarding the appropriate allocation of liability. Between August 2019 and April 2020, the Participants and SIFMA participated in numerous meetings (including with Commissioners and Commission staff) and exchanged extensive correspondence to address the Reporter Agreement's limitation of liability provisions and Industry Members' blanket objections to any limitation of liability whatsoever. During those discussions, the Participants attempted to be responsive to SIFMA's stated concerns, including risks related to personally identifiable information ("PII") and to the potential for misappropriation of a minority of Industry Members' proprietary trading algorithms. To facilitate those discussions as well as the launch of live CAT reporting, the Participants also revised FINRA CAT's testing procedures to enable Industry Members to test their connectivity to the CAT with obfuscated data rather than production data.

Although those discussions did not lead to a resolution, the Participants remain willing to work with Industry Members (and any other stakeholders) in good faith to resolve the parties' remaining differing perspectives. The Participants note, however, that prior to the filing of SIFMA's April 22, 2020 application for review of actions taken by CAT LLC and the Participants pursuant to Sections 19(d) and 19(f) of the Exchange Act (the "Administrative Proceeding"), the Participants provided SIFMA with term sheets for two proposals to revise the Limitation of Liability Provisions to address the industry's stated concerns.[7] SIFMA declined to respond to either proposal and did not offer any substantive counterproposals.[8] Throughout the entirety of the discussions regarding liability issues from August 2019 through April 2020, SIFMA's only "proposal" was to categorically reject any limitation of liability.

Notwithstanding SIFMA's historical unwillingness to negotiate regarding the substance and scope of a limitation of liability in the CAT Reporter Agreement, the Participants plan to reach out to SIFMA, following the filing of this letter, in a further attempt to resolve this dispute.

---

[5] Letter from Christopher A. Iacovella, American Securities Association to Vanessa Countryman, Secretary, U.S. Securities and Exchange Commission, at 3 (Jan. 29, 2021) (the "ASA Letter"), available at https://www.sec.gov/comments/4-698/4698-8311307-228499.pdf.

[6] Letter from Ellen Greene, SIFMA to Vanessa Countryman, Secretary, U.S. Securities and Exchange Commission, at 3 (Jan. 27, 2021) (the "SIFMA Letter"), available at https://www.sifma.org/wp-content/uploads/2021/01/SIFMA-comment-letter-File-No.-4-698.pdf.

[7] Those proposals were provided to the Commission on April 1, 2020. *See* April 1, 2020 Email from M. Simon to M. Kimmel.

[8] *See* Proposed Amendment at 3, available at https://www.catnmsplan.com/sites/default/files/2020-12/12.18.2020-Proposed-Amendment-to-the-CAT-NMS-Plan.pdf.

2) Settlement of the Administrative Proceeding

Five comment letters appear to suggest—incorrectly—that the settlement of the Administrative Proceeding somehow resolved the question of whether the Limitation of Liability Provisions should be included in the Reporter Agreement (and the Reporting Agent Agreement).[9] Simply put, that is not true, and the record is precisely to the contrary. The settlement of the Administrative Proceeding specifically contemplated that the Participants would request that the Commission address the proper allocation of liability following notice and comment.[10] SIFMA acknowledged this understanding publicly in its press release announcing the settlement of the Administrative Proceeding, noting that "[t]he SROs further agreed not to impose any limitation of liability language in the Reporter Agreement without first proposing a rule and going through the formal public notice, comment and approval process with the SEC."[11] By filing the Proposed Amendment—as specifically contemplated by the settlement of the Administrative Proceeding—the Participants have done just that, and provided all interested constituencies an opportunity to comment on the Limitation of Liability Provisions.[12]

---

[9] *See* SIFMA Letter at 4; Letter from Daniel Keegan, Citi to Vanessa Countryman, Secretary, U.S. Securities and Exchange Commission, at 2 (Feb. 25, 2021) (the "Citi Letter"), available at https://www.sec.gov/comments/4-698/4698-8419819-229522.pdf); Letter from Peggy L. Ho, LPL Financial to Vanessa Countryman, Secretary, U.S. Securities and Exchange Commission, at 1 (Jan. 27, 2021) (the "LPL Financial Letter"), available at https://www.sec.gov/comments/4-698/4698-8298412-228298.pdf; Letter from Joanna Mallers, FIA Principal Traders Group to Vanessa Countryman, Secretary, U.S. Securities and Exchange Commission, at 2 (Feb. 8, 2021) (the "FIA PTG Letter"), available at https://www.sec.gov/comments/4-698/4698-8345389-228979.pdf; Letter from Stephen John Berger, Citadel Securities to Vanessa Countryman, Secretary, U.S. Securities and Exchange Commission, at 1 (Feb. 23, 2021) (the "Citadel Letter"), available at https://www.sec.gov/comments/4-698/4698-8411798-229501.pdf).

[10] The settlement agreement resolving the Administrative Proceeding stated that "CAT LLC and the Participants agree not to require an Industry Member to enter into any CAT Reporter Agreement…that includes any limitation of liability provision as a condition of such Industry Member submitting CAT Data to the CAT System, **without having initiated a proposed rule-making pursuant to Section 19(b) of the Securities Exchange Act of 1934 or proposed plan amendment pursuant to Rule 608 of Regulation NMS**, which filing shall be subject to notice and comment after filing with the Commission… ." (emphasis added).

[11] SIFMA Statement on Settlement on CAT Reporter Agreement (May 13, 2020), available at https://www.sifma.org/resources/news/sifma-statement-on-settlement-on-cat-reporter-agreement/. Indeed, one of SIFMA's principal arguments in the Administrative Proceeding was that any limitation of liability in the Reporter Agreement must be approved through a rulemaking process. *See, e.g.*, *In re SIFMA*, Admin. Proc. No 3-19766, SIFMA Memorandum of Law in Support of Motion to Stay (Apr. 22, 2020) at 15 (arguing that "the standards, policies and practices that the SROs seek to impose in the CRA may only be established by an appropriate rule-making process, including an opportunity for the public to 'submit written data, views, and arguments'").

[12] The parties did not file the settlement agreement with the Commission in support of their May 14, 2020 joint request to dismiss the Administrative Proceeding. To the extent the Commission would consider it useful to review the agreement, the Participants are prepared to produce it.

B. Industry Standards Regarding Limitations of Liability

Several commenters expressed the view that the Limitation of Liability Provisions are inconsistent with industry standards.[13] These commenters assert that: 1) certain SRO liability rules provide Industry Members with a broad right to recover damages from the Participants and 2) any limitation of liability in relation to CAT Data should contain various exclusions (e.g., gross negligence and bad faith). Neither of these comments finds any support in the historical allocation of liability between the Participants and Industry Members, particularly where, as here, the Participants are implementing a regulatory mandate pursuant to SEC rule.

Additionally, certain Industry Members argue that industry standards provide that the party in possession of data bears all risk associated with a potential breach. As discussed below, the Participants are not aware of any basis for this purported principle (nor did any commenters offer any basis)—particularly in the context of a regulatory reporting system—and it is telling that several of the commenters who advocate for it generally disclaim liability in connection with sensitive data that *they* possess.

1) Self-Regulatory Organization Rules Governing Liability

Based on a comparison between the Limitation of Liability Provisions in the Proposed Amendment and "existing exchange rules that limit SRO liability," one commenter asserts that the Proposed Amendment is "completely out of line with industry standards."[14] That is not the case. As discussed in the Proposed Amendment, the exchanges have adopted rules—uniformly approved by the Commission as consistent with the Exchange Act—that broadly limit their liability to Industry Members.[15] The Proposed Amendment, which limits the liability of CAT LLC, the Participants, and FINRA CAT to Industry Members, is consistent with those securities exchanges' rules.[16]

While SIFMA correctly points out that certain exchange rules permit Industry Members to recover limited categories of damages, the SIFMA Letter omits that those rules generally vest the SROs with the discretion—not the obligation—to compensate harmed Industry Members. For example, Cboe Exchange, Inc. Rule 1.10(b) (discussed in the SIFMA Letter) provides that "the Exchange may, **in its sole discretion**, compensate one or more Trading Permit Holders for their losses …."[17]

---

[13] *See, e.g.*, SIFMA Letter at 7-8; Letter from Matthew Price, Fidelity Investments to Vanessa Countryman, Secretary, U.S. Securities and Exchange Commission, at 1, 2 (Feb. 2, 2021) (the "Fidelity Letter"), available at https://www.sec.gov/comments/4-698/4698-8343750-228940.pdf.

[14] SIFMA Letter at 7.

[15] *See* Proposed Amendment at 5-6, n.14, n.15.

[16] *Id.*

[17] Cboe Exchange, Inc., Rule 1.10(b) (emphasis added); *see also* SIFMA Letter at 7.

Many other exchanges have a compensation mechanism that affords the exchange discretion in determining whether to compensate Industry Members.[18]

The Participants also note that one of the term sheets that the Participants provided to SIFMA in an attempt to resolve the liability disagreement provided for a discretionary compensation mechanism modeled on SRO rules—a proposal similar to the one for which SIFMA now appears to advocate in its comment letter.[19] SIFMA rejected that proposal out of hand.

The SIFMA Letter also omits that the Commission-approved rules that afford the SROs the discretion to compensate Industry Members apply in very limited circumstances—namely, for system failures that impact the execution of individual orders. By way of example, Investors Exchange LLC Rule 11.260(d) provides that "the exchange may compensate members for losses directly resulting from the systems' actual failure to correctly process an order, message, or other data, provided the exchange has acknowledged receipt of the order, message or data."[20] The rules of the other Participants also generally restrict the circumstances under which the SROs retain discretion to compensate Industry Members.[21] And while there are minor variations in the precise scope of each SRO's liability rules, none contemplates SRO liability under the circumstances for which SIFMA advocates here: "catastrophic" damages resulting from the theft of Industry Members' proprietary trading algorithms.[22]

Finally, the Participants note that while they considered the scope of exchange liability rules in preparing the Proposed Amendment, their assessment that the Limitation of Liability Provisions fall squarely within industry norms was based on a broader consideration of provisions that limit liability to Industry Members. As discussed in the Proposed Amendment, the Participants considered that NMS facilities that receive transaction data utilize broad limitations of liability that protect both the actual facility and its constituent self-regulatory organizations.[23] The Participants also considered the longstanding allocation of liability between Industry Members and self-regulatory organizations in connection with reporting data to OATS, which has functioned as a comprehensive audit trail for equity securities since 1998. The Limitation of Liability Provisions in the Proposed Amendment are substantively identical to the liability provisions to which virtually

---

[18] *See* Box Exchange LLC, Rule 7230(e); Investors Exchange LLC, Rule 11.260(d); Long-Term Stock Exchange, Inc., Rule 11.260(d); MEMX LLC, Rule 11.14(d),(g); Nasdaq Equity, Rule 2: Market Participants, Section 17(b); Nasdaq Marketplace Rules, Rule 4626(b); and NYSE LLC, Rule 18.

[19] *See* April 1, 2020 Email from M. Simon to M. Kimmel, attachment entitled Proposed Terms Regarding Compensation to Industry Members in the Event of a CAT Data Breach–Funding Approach; SIFMA Letter at 7.

[20] Investors Exchange LLC, Rule 11.260(d).

[21] *See* Box Exchange LLC, Rule 7230(e); Cboe Exchange, Inc., Rule 1.10(b); Long-Term Stock Exchange, Inc., Rule 11.260(d); MEMX LLC, Rule 11.14(d),(g); Nasdaq Equity, Rule 2: Market Participants, Section 17(b); Nasdaq Marketplace Rules, Rule 4626(b); NYSE LLC, Rule 18; *see also* Miami International Securities Exchange LLC, Rule 527(b).

[22] *See* SIFMA Letter at 4.

[23] *See* Proposed Amendment at 7 (providing examples).

all Industry Members regularly agree in connection with OATS reporting.[24] The commenters who incorrectly opined that the Proposed Amendment is inconsistent with industry standards focused solely on SRO rules, which they incorrectly summarized, and did not consider other contexts in which contracts limit SROs' (as members of NMS plans) liability to Industry Members.[25]

2) Proposed Exclusions for Gross Negligence, Willful Misconduct, Bad Faith and Criminal Acts

SIFMA asserts that any liability limitation that the Commission ultimately approves "should not extend to willful misconduct, gross negligence, bad faith or criminal acts of CAT LLC, the SROs or their representatives or employees."[26] SIFMA's proposal runs counter to the SEC-approved rules of SROs that do not recognize exclusions similar to those that SIFMA advocates for here.[27] Importantly, the SRO rules that do contain categorical exclusions are generally modified by other rules that broadly prohibit Industry Members from suing the exchanges or their representatives, except for violations of the federal securities laws for which a private right of action exists.[28] Accordingly, even when SRO liability rules permit certain types of claims (e.g., gross negligence and willful misconduct), Industry Members are often prohibited from suing an SRO for damages unless that SRO's alleged gross negligence or willful misconduct also constituted a securities law violation for which Congress authorized a private right of action.[29] The Participants do not believe

---

[24] Despite commenters' attempts to distinguish OATS on the basis that it was created two decades ago, as discussed in the Proposed Amendment, Industry Members agree to the terms of the OATS limitation of liability provision on an ongoing basis. FINRA Rule 1013(a)(1)(R) requires all applicants for FINRA Membership to acknowledge the FINRA Entitlement Program Agreement and Terms of Use, which applies to OATS. Industry Members click to indicate that they agree to its terms—including its limitation of liability provision—every time they access FINRA's OATS system to report trade information (i.e., repeatedly over the course of a trading day for many Industry Members).

[25] Notably, no commenters have argued that the OATS limitation of liability provision—to which Industry Members agree every time they access FINRA's OATS system—is inconsistent with the Limitation of Liability Provisions in the Proposed Amendment. *See generally* SIFMA Letter; Letter from Thomas M. Merritt, Virtu Financial to Vanessa Countryman, Secretary, U.S. Securities and Exchange Commission (Jan. 27, 2021) (the "Virtu Letter"), available at https://www.sec.gov/comments/4-698/4698-8298023-228258.pdf; *see also* Craig M. Lewis, Ph.D., Economic Analysis of Proposed Amendment to National Market System Plan Governing the Consolidated Audit Trail, at 9-10 (Feb. 19, 2021) (the "Lewis Report"), available at https://www.sec.gov/comments/4-698/4698-8394069-229410.pdf). Although the SIFMA Letter and Virtu Letter discuss OATS reporting, those discussions focus on perceived differences between OATS and the CAT. *See* SIFMA Letter at 8; Virtue Letter at 4; *see also* Lewis Report at 9-10. The crux of SIFMA's and Virtu's argument is that because the CAT receives more data than OATS, the OATS limitation of liability should not inform the scope of the Limitation of Liability Provisions in the CAT Reporter Agreement. *Id.* The Participants are not aware of any rationale as to why the differences between the CAT and OATS should impact the appropriate allocation of liability, or why such differences would support shifting liability from Industry Members to regulators.

[26] *See* SIFMA Letter at 7-8.

[27] *See, e.g.*, Investors Exchange LLC, Rule 11.260; Long-Term Stock Exchange, Inc., Rule 11.260; Nasdaq Equities, Rule 4626; NYSE LLC, Rule 17.

[28] *See, e.g.*, BOX Exchange LLC, Rule 7230(d); Cboe Exchange, Inc., Rule 1.15; and Miami International Securities Exchange LLC, Rule 528.

[29] Cboe's liability rule that contains exclusions (e.g., gross negligence) was drafted and approved before courts made clear that Commission-approved rules can supersede state law that purports to limit parties' ability to contractually

that these provisions would provide for liability against the self-regulatory organizations in the event of a data breach.[30]

The Participants also note that contractual limitations of liability that protect the Participants from claims for damages in connection with other NMS plans and regulatory reporting facilities (including OATS) do not contain the exclusions that SIFMA advocates to be included in the CAT Reporter Agreement.[31] Commenters have not provided any reason to deviate from this longstanding precedent in the context of CAT reporting.

In addition to failing to find support within SRO liability rules or other contractually based liability limitations, SIFMA's proposal to exclude gross negligence, willful misconduct, bad faith, and criminal acts is not supported by Charles River's economic analysis. In concluding that a limitation of liability provision is appropriately included in the Reporter Agreement, Charles River determined that the disadvantages of allowing Industry Members to litigate against CAT LLC, the Participants, and FINRA CAT outweigh any benefits in part because of the substantial direct and indirect costs of litigation. As Charles River explained:

---

disclaim liability for gross negligence and willful misconduct. *See NASDAQ OMX Grp., Inc. v. UBS Secs., LLC*, 770 F.3d 1010 (2d Cir. 2014) (SRO rules on liability were exempt from New York law prohibiting insulation from gross negligence by contract). Cboe's rule was one of the earlier drafted SRO liability rules and served as a model for other SRO rules on liability containing exclusions that were drafted later. In the analogous context of SRO immunity, courts have long recognized the important policy rationale behind prohibiting Industry Members from suing the self-regulatory organizations—even for allegations of gross negligence or willful misconduct. *See, e.g.*, *DL Cap. Grp., LLC v. Nasdaq Stock Mkt., Inc.*, 409 F.3d 93, 98-99 (2d Cir. 2005) (declining to create exception for fraud because it is "hard to imagine the plaintiff (or plaintiff's counsel) who would—when otherwise wronged by an SRO but unable to seek money damages—fail to concoct some claim of fraud in order to try and circumvent the absolute immunity doctrine"); *In re Series 7 Broker Qualification Exam Scoring Litig.*, 548 F.3d 110, 115 (D.C. Cir. 2008) ("Where courts accord immunity to SROs, the protection has been absolute.") (citing *Desiderio v. NASD*, 191 F.3d 198, 208 (2d Cir. 1999) (declining to create exception for bad faith); *Sparta Surgical Corp. v. NASD*, 159 F.3d 1209, 1215 (9th Cir. 1998) (declining to create exception for bad faith or gross negligence), *abrogated in part on other grounds by Merrill Lynch, Pierce, Fenner & Smith Inc. v. Manning*, 136 S. Ct. 1562 (2016)); *see also Citadel Sec. LLC v. Chicago Bd. Options Exch., Inc.*, No. 16 C 9747, 2018 WL 5264195, at *4 (N.D. Ill. Oct. 23, 2018) (finding defendants were immune from plaintiff's claims, including claims for willful misconduct and gross negligence); *DGM Invs., Inc. v. N.Y. Futures Exch., Inc.*, No. 01 CIV. 11602 (RWS), 2002 WL 31356362, at *5 (S.D.N.Y. Oct. 17, 2002) (claims for gross negligence, bad faith, and *respondeat superior* against the New York Futures Exchange were preempted by the CEA because the claims were based on allegations that the defendants "failed to fulfill their obligation to regulate the market").

[30] The SIFMA Letter's discussion of industry standards also omits that Commission-approved exchange rules generally require Industry Members to pay attorneys' fees in the event that they commence litigation against an exchange and do not prevail. *See, e.g.*, CBOE, Rule 2.5; BOX Exchange LLC, Rule 1060; Investors Exchange LLC, Rule 2.170(a)(4); Long-Term Stock Exchange, Inc., Rule 2.170(a)(4); MEMX LLC, Rule 2.6(a)(4); Miami International Securities Exchange LLC, Rule 1205.

[31] *See, e.g.*, FINRA Entitlement Program Terms of Use, available at https://www.finra.org/sites/default/files/Entitlement_Program_Privacy_Statement.pdf; Options Price Reporting Authority, Vendor Agreement, available at https://assets.website-files.com/5ba40927ac854d8c97bc92d7/5c6f058889c3684b7571a552_OPRA%20Vendor%20Agreement%20100118.pdf; Options Price Reporting Authority Subscriber Agreement, available at https://assets.website-files.com/5ba40927ac854d8c97bc92d7/5bf421d078a39dec23185180_hardcopy_subscriber_agreement.pdf.

> It is well-understood that litigation in general is an expensive and highly uncertain process. This holds with particular persuasiveness for the new, highly technical, and rapidly changing area of cyber security. The level of expertise required to establish what went wrong, who was responsible, and then the calculation of relevant losses is extremely high, placing large information burdens on the triers-of-fact. In the case of CAT LLC, there would be an additional burden of demonstrating either that the SEC's cyber security mandates were inadequately implemented or were insufficient to the task. Discovery in such litigation also runs the risk of revealing crucial cyber security information to malicious actors. There are, therefore, substantial unquantifiable direct costs associated with litigating cyber security breaches at the CAT.[32]

If the Commission amends the Limitation of Liability Provisions to exclude certain categories of conduct, any CAT Data breach is likely to generate litigation in which allegedly harmed parties attempt to demonstrate that those exclusions apply—regardless of the putative defendants' actual culpability (if any). Although the Participants, CAT LLC, and FINRA CAT may ultimately be found not liable, litigation would be expensive and time-consuming, distract the Participants from their important regulatory oversight mandate (as ordered by the Commission), and open the doors of discovery to potentially malicious actors.[33] Further, litigating even these limited claims increases the costs of operating CAT—costs that would be borne by the Participants and Industry Members alike. In short, a limitation of liability with any categorical exclusions could result in many of the same economic harms that would occur in the absence of any limitation of liability at all.

The Commission should also consider that certain relief ordered in litigation could interfere with the Commission's oversight of the CAT (i.e., by imposing mandates or restrictions that constrain the Commission's policy choices). The Proposed Amendment affords the Commission complete oversight of CAT's cybersecurity and enables the Commission to balance the full range of relevant considerations in fashioning any post-breach remedies. In contrast, under Industry Members' preferred approach, the Commission would have to share that jurisdiction with the courts, whose rulings could diverge from Commission priorities in meaningful ways.

Finally, because the Commission's regulatory enforcement regime and the potential for severe reputational harm already sufficiently incentivize the Participants to not engage in bad faith, recklessness, gross negligence, and intentional misconduct, commenters' proposed exclusions would not result in any meaningful improvement to the CAT's cybersecurity.[34] Considering the lack of any benefit and the potential for substantial costs, the Commission should decline SIFMA's invitation to amend the Limitation of Liability Provisions to create categorical exclusions.

---

[32] *See* Appendix B to Proposed Amendment ("Appendix B") at 46.

[33] *Id.*

[34] *See, e.g.*, *infra* at E(4).

3) Control of CAT Data

Six commenters opined that the Limitation of Liability Provisions are inappropriate because of the now-familiar refrain that the Participants and FINRA CAT "control" the CAT Data.[35] These commenters base their position on a purported belief that the party who possesses the data should bear all risk associated with a data breach—even if that party is a regulator acting pursuant to SEC mandate. For example, one commenter asserts that "[a]ligning 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."[36] None of these comment letters offers any explanation, let alone one rooted in the Exchange Act, as to why this purported principle is applicable to a regulatory program with Commission-mandated reporting.

Additionally, as discussed in the Proposed Amendment, Industry Members routinely disclaim liability to their underlying customers despite controlling sensitive data that could be compromised during a data breach. The Participants also note that certain commenters who have advocated for this principle broadly disclaim liability to their *own* retail customers—despite those same commenters having "control" over sensitive data that would harm customers if compromised via a data breach.[37] For example, Fidelity Investments Inc., which manages over $9.3 trillion in customer assets, mandates that its brokerage customers agree that it is not responsible "for any losses" that customers suffer as a result of a cyber breach (among other causes) and broadly disclaims liability for all "direct, indirect, incidental, or consequential damages."[38]

The Participants do not believe that securities industry norms support the principle that the party in possession of data should bear liability in the event of a data breach. That is particularly true where, as here, the parties in possession of the data (i.e., the Participants and FINRA CAT) are acting in regulatory capacities pursuant to Commission rules.

* * *

The Participants maintain that the Limitation of Liability Provisions in the Proposed Amendment are well within industry norms as demonstrated by a comparison to the allocation of liability between Industry Members and SROs in every other regulatory context—including NMS Plans,

---

[35] *See* SIFMA Letter at 4-5 and *generally*; Virtu Letter at 2-3; Fidelity Letter at 2; Citi Letter at 4; FIA PTG Letter at 1; Letter from Thomas Tremaine, Raymond James to Vanessa Countryman, Secretary, U.S. Securities and Exchange Commission, at 2 (Feb. 8, 2021) (the "Raymond James Letter"), available at https://www.sec.gov/comments/4-698/4698-8347733-229000.pdf; *see also* Lewis Report at 5-7.

[36] SIFMA Letter at 4.

[37] *See* Proposed Amendment at 8, n.26 (citing examples of Industry Members liability limitations).

[38] *Compare* Fidelity Account Customer Agreement, at 11, 13, available at https://www.fidelity.com/bin-public/060_www_fidelity_com/documents/customer-service/updated-agreements/Fidelity-Account-Customer-Agreement.pdf; *with* Fidelity Letter at 2.

regulatory reporting facilities, and SRO rules—and the liability provisions that Industry Members utilize to protect themselves when they possess sensitive customer and transaction data.[39]

C. The Cybersecurity of the CAT

Commenters raised several purported concerns about the use of CAT Data, including concerns about bulk downloading and PII. Commenters also offered suggestions regarding FINRA CAT and the Participants' controls designed to prevent internal cyber breaches. None of those comments provides a basis upon which to disregard the historical allocation of liability between Industry Members and their primary regulators. One commenter also asserted, incorrectly, that Industry Members are not able to provide feedback to the Participants or the Commission regarding the CAT's cybersecurity. The Participants address each of these comments below.

1) Bulk Downloading of CAT Data

Several commenters indicated that the risks presented by a potential data breach are increased to the extent that the SROs engage in bulk downloading.[40] By way of example, one commenter states that "[a]ny of the SROs that jointly operate the CAT currently may download onto their servers vast amounts of customer and trading data … ."[41] As a preliminary matter, this comment misstates the scope of data that is subject to bulk downloading. The Participants are only authorized to bulk download trading data—not customer data.[42] As the Commission has recognized, "no customer-

---

[39] The Commission tacitly endorsed the longstanding allocation of liability between Industry Members and the Participants as recently as December 9, 2020—approximately one week before the Proposed Amendment was filed—when the Commission referenced contractual limitation of liability for consolidators of NMS information (like the CAT) in its rulemaking on market data infrastructure. *See* SEC, Market Data Infrastructure, Release No. 34-90610; File No. S7-03-20, at 668 (Dec. 9, 2020), available at https://www.sec.gov/rules/final/2020/34-90610.pdf (stating that potential liability concerns are not a significant barrier to entry for competing consolidators of NMS information because they can "attempt to limit their potential liability from systems issues through contractual agreements with their subscribers, similar to provisions that data providers currently include in their subscriber agreements."), citing CTA Plan Professional Subscriber Agreement, available at https://www.nyse.com/publicdocs/ctaplan/notifications/trader-update/Professional%20Subscriber%20Agreement.pdf; UTP Plan Subscriber Agreement, available at http://www.utpplan.com/DOC/subagreement.pdf; Nasdaq Global Subscriber Agreement, available at: http://www.nasdaqtrader.com/content/AdministrationSupport/AgreementsData/subagreemstandalone.pdf; ICE Data Services and Software Services Agreement, available at: https://www.theice.com/publicdocs/agreements/ICE_Data_Services_Agreement.pdf.

[40] *See* SIFMA Letter at 5; Letter from Kelvin To, Data Boiler Technologies, LLC to Vanessa Countryman, Secretary, U.S. Securities and Exchange Commission, at 4 (Jan. 27, 2021) (the "Data Boiler Letter"), available at https://www.sec.gov/comments/4-698/4698-8311309-228460.pdf; Citadel Letter at 6; *see also* Virtu Letter at 2.

[41] SIFMA Letter at 5.

[42] *See* CAT NMS Plan, Appendix C at 35 ("PII such as SSN and TIN will not be made available in the general query tools, reports, or bulk data extraction."); CAT NMS Plan, Appendix D at 33 ("The CAT must capture and store Customer and Customer Account Information in a secure database physically separated from the transactional database."); *Id.* at 14 ("PII data must not be included in the result set(s) from online or direct query tools, reports or bulk data extraction.").

related information, including PII, will be included in response to queries of the broader order and transaction database, nor will it be available in bulk extract form."[43]

As discussed above, several commenters also raised concerns with respect to the cybersecurity of the Participants' systems that might store CAT Data. One commenter stated that "the SEC has assessed whether 'the existing cyber security framework is adequate' only as to the CAT databases. The Commission has made no such conclusion with respect to the Participants' security."[44] The Participants note that FINRA CAT has adopted and implemented policies, procedures, systems, and controls to address cybersecurity concerning bulk downloading of CAT Data by the Participants. The Participants also note that any individual SRO that engages in bulk downloading:

> must have policies and procedures regarding CAT Data security that are comparable to those implemented and maintained by the Plan Processor for the Central Repository, and that each Participant must certify and provide evidence to the CISO that its policies and procedures for the security of CAT Data meet the same security standards applicable to the CAT Data that is reported to, and collected and stored by, the Central Repository.[45]

Finally, as with FINRA CAT, the Participants' cybersecurity protocols are subject to the Commission's regulatory oversight regime, including its examination and enforcement functions.

2) Misuse of CAT Data by Regulatory Personnel

Four commenters expressed concerns regarding a breach or misuse of CAT Data that originates from within FINRA CAT or the Participants. Because those comments were raised in the context of a critique of Charles River's methodology, the Participants will principally respond to those comments in the section of this submission addressing comments on the Proposed Amendment's economic analysis.[46] The Participants note, however, that FINRA CAT's and the Participants' robust cybersecurity protocols are designed to prevent and detect both external and internal security threats.[47]

One commenter expressed concerns regarding its belief "that roughly 3,000 random individuals will have access to the highly sensitive information under the CAT at any given time."[48] The Participants reiterate that FINRA CAT's and the Participants' robust cybersecurity regimes are designed to address potential internal security threats. Moreover, access to CAT Data is not "random;" rather, it is granted strictly on a need-to-know basis to Commission and other regulatory

---

[43] SEC, Order Approving CAT NMS Plan at 290.

[44] Citadel Letter at 8.

[45] SEC, Order Approving CAT NMS Plan at 252-53.

[46] *Infra* at D(1).

[47] *See* CAT NMS Plan, Section 6.1(g); *see also* CAT NMS Plan, Appendix D at 12-13 ("The Plan Processor must develop and maintain policies and procedures reasonably designed to prevent, detect, and mitigate the impact of unauthorized access or usage of data in the Central Repository… A Role Based Access Control ('RBAC') model must be used to permission user with access to different areas of the CAT system.").

[48] ASA Letter at 2.

users only (most of whom will have access only to transaction data), and individuals who are provided access and must successfully undergo comprehensive background checks.[49]

3) Personally Identifiable Information

One commenter opined that the risk of a data breach is heightened by the collection of PII.[50] The Participants appreciate concerns regarding customer data and remain vigilant in taking all appropriate cybersecurity measures to protect customer information (and all CAT Data). Further, the Commission granted the Participants' requested relief to no longer require that Industry Members report social security numbers, dates of birth, and full account numbers for individual retail customers.[51] The Participants note that this exemptive relief significantly reduces the risk of a breach involving customer data, and that the customer data stored in the CAT is comparable to the data reported to other regulatory reporting facilities, for which the Commission has previously approved limitations of liability.[52]

4) Input from Industry Members Regarding the CAT's Cybersecurity

One commenter incorrectly stated that Industry Members "have no input into the security and risk mitigation measures that CAT LLC and the Plan Processor should implement … ."[53] Another commenter argued that "[a]lthough the industry has visibility and influence over how broker-dealers report data to the CAT, there is no visibility, through the Advisory Committee or otherwise, into the security aspects of the CAT" and asserted that "industry members should be added to the CAT Security Working Group."[54]

---

[49] SEC, Order Approving CAT NMS Plan at 715 ("[T]he Commission is amending the Plan to require that the Participants conduct background checks for the employees and contractors of the Participants that will use the CAT System, and to require that the Participants provide the Commission with an evaluation of the information security program to ensure that the program is consistent with the highest industry standards for the protection of data."). The Participants also note that most active users of the CAT will have access only to transaction data—not customer data. *See* CAT NMS Plan, Appendix C at 15.

[50] ASA Letter at 1-2.

[51] SEC, 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 (Mar. 17, 2020). Additionally, while discussing an amendment to formalize the conditions of this exemptive relief, the Commission noted that the proposed amendment would result in "removing sensitive PII from CAT reporting requirements in accordance with the March 2020 PII Exemption Order…" and a CAT "operating without sensitive PII." *See* Chairman Jay Clayton, Director Brett Redfearn and Senior Policy Advisor Manisha Kimmel, SEC, Update on the Consolidated Audit Trail: Data Security and Implementation Progress (Aug. 21, 2020), available at https://www.sec.gov/news/public-statement/clayton-kimmel-redfearn-nms-cat-2020-08-21.

[52] *See* Proposed Amendment at 9.

[53] Virtu Letter at 2. Another commenter made similar incorrect statements regarding the role of Industry Members with respect to CAT's cybersecurity. *See* Citi Letter at 2 (stating that CAT has been developed "exclusively" by the Participants).

[54] Citadel Letter at 9.

Industry Members have had extensive opportunities to provide input regarding the CAT's cybersecurity at every stage of the development and operation of the CAT. Beginning in 2012, Industry Members provided feedback regarding cybersecurity issues in connection with the process of commenting on then-proposed Rule 613 of Regulation NMS.[55] Prior to the approval of the CAT NMS Plan, Industry Members provided feedback on the Plan's cybersecurity requirements through the Development Advisory Group. Following approval of the CAT NMS Plan, Industry Members continued to provide feedback regarding the CAT's cybersecurity through the Advisory Committee, which serves as a forum for Industry Members to raise any cyber-related suggestions. Finally, Industry Members—and other interested constituencies—may directly petition the Commission to impose additional requirements on FINRA CAT and the Participants and may provide comments on any proposals offered by the Commission.

Another commenter proposed 26 specific cyber "compliance requirements" for the Participants' and the Commission's consideration.[56] That proposal, which was copied verbatim from that commenter's submission in response to the Proposed Amendments to the National Market System Plan Governing the Consolidated Audit Trail to enhance data security published on August 21, 2020,[57] is beyond the scope of the Proposed Amendment, which relates solely to the allocation of liability in the event of a CAT Data breach. Without responding to each of the 26 suggestions individually, the Participants note that FINRA CAT has implemented robust controls to protect the security and confidentiality of CAT Data and that the Commission has repeatedly concluded that the CAT NMS Plan incorporates "robust security requirements" that "provide appropriate, adequate protection for the CAT Data."[58] The Participants are not aware of any basis to challenge the Commission's conclusion (and commenters have not offered any). Additionally, the Participants, along with FINRA CAT, regularly assess the security of the CAT and consider whether and how CAT Data security can be enhanced on an ongoing basis. Finally, although the Participants welcome any constructive suggestions from Industry Members regarding the CAT's cybersecurity, it is the responsibility of the regulators (the Participants and ultimately the Commission, as the regulator of the SROs)—and not the regulated entities—to determine the

---

[55] *See* SEC, Order Approving CAT NMS Plan at 914 (summarizing changes to proposed Rule 613 in response to comments).

[56] Data Boiler Letter at 2-4.

[57] *See* Letter from Kelvin To, Data Boiler Technologies, LLC to Vanessa Countryman, Secretary, U.S. Securities and Exchange Commission, Release No. 34-89632; File No. S7-10-20, at 3-4 (Nov. 30, 2020), available at https://www.sec.gov/comments/s7-10-20/s71020-8068693-225956.pdf.

[58] SEC, Order Approving CAT NMS Plan at 715; *see also* SEC, Proposed Amendments to the National Market System Plan Governing the Consolidated Audit Trail to Enhance Data Security, Release No. 34-89632; File No. S7-10-20, at 10 (Aug. 21, 2020) (the "Data Security Proposal"), available at https://www.sec.gov/rules/proposed/2020/34-89632.pdf, 85 Fed. Reg. 65990 at 65991 (Oct. 16, 2020), available at https://www.govinfo.gov/content/pkg/FR-2020-10-16/pdf/2020-18801.pdf ("CAT Data reported to and retained in the Central Repository is thus subject to what the Commission believes are stringent security policies, procedures, standards and controls.").

CAT's required security measures in a manner consistent with the Exchange Act and other applicable statutes, rules, and regulations.[59]

D. Economic Analysis of Liability Issues

Certain commenters opined that particular hypothetical breach scenarios were not addressed in Charles River's White Paper and disagreed with Charles River's analysis of the costs and benefits of allowing Industry Members to litigate against their regulators in the event of a CAT Data breach. Commenters also argued that CAT LLC's and certain Participants' responses to the Commission's August 2020 CAT Data Security Proposal demonstrate that the Limitation of Liability Provisions are inappropriate. Finally, one commenter suggested that the Commission did not consider certain risks associated with a CAT Data breach when it approved the CAT NMS Plan. The Participants address each of these comments below.

1) Charles River's Methodology and Conclusions

Charles River's White Paper contained two principal analyses. First, Charles River conducted a "scenario analysis" in which it identified specific hypothetical breaches and assessed "the relative difficulty of implementation, relative frequency, and conditional severity of each."[60] Second, Charles River considered whether the cyber risk presented by the CAT should be addressed by regulation, litigation, or a combination of both approaches.[61]

Four commenters opined that Charles River's scenario analysis did not address certain categories of hypothetical data breaches, including breaches that originate from within FINRA CAT or the Participants.[62] For example, one commenter opines that the White Paper "is focused almost exclusively on an assessment of an external malicious actor's ability to 'hack' into one or more of the CAT databases."[63] These comments misconstrue Charles River's analysis. In analyzing the various scenarios discussed in the White Paper, Charles River did not make any assumptions regarding the identity of potential bad actors or where they may work.[64] Moreover, Charles River explicitly stated in its report that it was not attempting to predict every possible scenario and "recognize[d] that cyber-attacks on the CAT could vary from the scenarios we hypothesize."[65] Charles River's scenario analysis was illustrative, not exhaustive, and "offered … to provide a

---

[59] As the Commission recently recognized, it is not the role of regulated entities (i.e., Industry Members) to provide oversight regarding the cybersecurity of their regulators (i.e., the Participants). *See* Data Security Proposal at 246 ("[T]he Commission is the regulator of the Participants, and the Commission oversees and enforces their compliance with the CAT NMS Plan. To impose obligations on the Commission under the CAT NMS Plan would invert this structure, raising questions about the Participants monitoring their own regulator's compliance with the CAT NMS Plan.").

[60] Appendix B at 2.

[61] *Id.*

[62] SIFMA Letter at 9; Raymond James Letter at 2; Citadel Letter at 6; Virtu Letter at 5.

[63] Citadel Letter at 6.

[64] *See* Appendix B at 2.

[65] *Id.*

framework to assess the economic exposures that flow from the gathering, storage, and use of CAT data."[66] As discussed in the White Paper, the scenario analysis indicated that, in light of the CAT's extensive cybersecurity (among other reasons), most potential breaches are relatively low-frequency events because they are either difficult to implement, unlikely to be meaningfully profitable, or both.[67]

The second component of Charles River's analysis is an economic assessment of the costs and benefits of including a limitation of liability provision in the Reporter Agreement. As an initial matter, the Participants note that Charles River's analysis of whether the risk of a potential data breach is most effectively addressed through *ex ante* regulation or *ex post* litigation is independent from Charles River's scenario analysis. From an economic perspective, the issue of whether Industry Members should be afforded a novel private right of action against the Participants depends solely on the costs, benefits, and incentives of adding that feature to the SEC's existing regulatory regime.[68] The scenario analysis—which assesses relative risks of specific types of breaches—does not speak to those issues. Thus, Charles River's conclusion that allowing Industry Members to litigate against CAT LLC, the Participants, and FINRA CAT would provide minimal benefits while imposing substantial costs is not undermined to the extent that commenters identify potential breaches that were not included in Charles River's scenario analysis.

Three commenters disagreed with Charles River's assessment of the costs and benefits of a limitation of liability provision on the basis that the White Paper did not consider the costs to individual Industry Members in the event of a CAT Data breach. For example, one commenter asserts that "the corollary missing from the CRA Report is that the liability for a potentially catastrophic loss would then be shifted to individual Industry Members."[69] These comments are based on a fundamental misunderstanding of the relevant economic principles. As Charles River points out, the crux of the analysis is whether the risks of a particular economic activity—in this case, the use of CAT Data for regulatory purposes—are best managed through *ex ante* regulation or *ex post* litigation (or a combination of both approaches). That analysis largely turns on identifying the most effective and efficient mechanisms for incentivizing the relevant economic actors—in this case, CAT LLC, the Participants, and FINRA CAT—to take appropriate precautions. As discussed in the White Paper, Charles River's analysis demonstrates that: 1) the extensive regulatory regime that the SEC has enacted creates appropriate incentives for the Participants to take sufficient cybersecurity precautions, and 2) allowing Industry Members to litigate against the Participants would create substantial costs across the securities markets without any corresponding benefit.[70]

One commenter argues that if the Participants do not "assum[e] liability for issues the SROs themselves cause, these SROs are not adequately incentivized to prevent harm from their actions

---

[66] *Id.*

[67] *Id.* at 18-32.

[68] *Id.* at 4-5.

[69] SIFMA Letter at 10.

[70] *See* Appendix B at 53-54.

in the way that other market participants are."[71] The Participants note that this unsupported assertion is contradicted by Charles River's analysis, which demonstrates that the Commission's existing regulatory enforcement regime (among other factors, including potential reputational harm for various parties and the need to use the CAT for their own regulatory purposes), creates strong incentives for the Participants to ensure that the CAT is secure.[72] Additionally, the commenters' argument that limitations of liability undermine incentives to take appropriate cybersecurity precautions is belied by the commenters' decisions to impose limitations of liability on their underlying retail customers.

Three commenters expressed concerns that certain categories of potential breaches might result in substantial damages to individual Industry Members.[73] The Participants note that no commenter offered any economic argument as to why the longstanding historical allocation of liability should not apply to CAT reporting, and that the risks associated with "black swan" events should be shifted from regulated entities (Industry Members) to regulators (the Participants and the SEC). As discussed in the Proposed Amendment, it is difficult to imagine how CAT LLC could ensure its solvency—as required by the CAT NMS Plan—without limiting its liability to Industry Members, particularly in relation to "black swan" data breaches. The Participants reiterate that CAT LLC has obtained the maximum extent of cyber-breach insurance coverage available at the time and are willing to discuss once again with Industry Members (and the Commission) how that coverage might be used to compensate parties harmed by a potential data breach.[74]

Finally, one commenter questioned the independence of Charles River and accused the White Paper of delivering a "pre-determined conclusion."[75] These criticisms are unfounded. The Participants note that Charles Rivers' sole assignment was to "assess the economic aspects of a potential cyber breach as a result of the operation of the Consolidated Audit Trail."[76] The Participants also note that the Charles River team that worked on this engagement includes: 1) economists who have worked extensively in risk analysis and financial markets in academic, litigation, and regulatory settings (including the dean of a noted college of business who holds a named chair in risk management and insurance) and 2) business consultants with deep knowledge and experience in the operations of financial markets (including fraud and other failures of those markets) and cybersecurity.[77]

---

[71] Citi Letter at 3; *see also* Citadel Letter at 7.

[72] Appendix B at 3.

[73] *See* SIFMA Letter at 4; FIA PTG Letter at 2; ASA Letter at 1-2.

[74] *See infra* at Section G.

[75] ASA Letter at 2-3.

[76] Appendix B at 1.

[77] *See* Appendix B at 57-60; *see also* 61-68 (description of Charles Rivers' Research Program and Bibliography).

2) August 2020 CAT Data Security Proposal

Three commenters opined that the Limitation of Liability Provisions are inappropriate[78] in light of CAT LLC's and certain Participants' responses to the Commission's August 21, 2020 CAT Data Security Proposal.[79] According to one commenter, the Participants' responses highlight "the policy risks of de-linking control and liability."[80]

These comments, which imply that the Commission's regulatory regime is insufficient to properly incentivize the Participants, are based on a fundamental misunderstanding of the applicable economic principles. Under the regulatory regime that the Commission has enacted to govern the CAT, all interested parties—including CAT LLC and the Participants—provide feedback to the Commission regarding any proposals to the CAT's cybersecurity. While it is beyond dispute that the Participants have implemented robust protections regarding CAT Data—indeed, the Commission itself has observed that the CAT NMS Plan incorporates "robust security requirements" that "provide appropriate, adequate protection for the CAT Data"[81]—the Commission will ultimately decide whether to adopt any of the additional measures in its Data Security Proposal after all interested constituencies (including Industry Members) have an opportunity to comment. As Charles River explains, this robust process is a feature of an effective regulatory regime and provides further support for the Participants' position that litigation would not provide any additional benefits to the CAT's cybersecurity.[82]

The Commission, unlike the courts, has the substantive expertise and an understanding of stakeholder interests necessary to balance *all* appropriate factors in identifying (and over time, re-evaluating) the CAT's cybersecurity needs. Litigation regarding CAT's cybersecurity would compromise the Commission's comprehensive oversight authority and potentially result in court orders that constrain the Commission's policy options or strike a suboptimal balance among competing priorities. For example, a court might interpret the standard of care as requiring CAT infrastructure changes that would impede other CAT priorities such as rapid query response time and prompt implementation of new capabilities. The Commission is well-equipped to consider and address these tradeoffs; courts, by contrast, are not.

One commenter opined that the "time needed to develop, approve, and publish" data security amendments like the Data Security Proposal indicates that "regulation can[not] keep pace with data security issues and motivate behavior."[83] This comment is also based on a misunderstanding of the relevant economic principles. As Charles River explains, the deliberate nature of the amendment process—which affords all constituencies (including Industry Members) the opportunity to provide feedback and allows the Commission to be the ultimate arbiter of

[78] Virtu Letter at 4-5; SIFMA Letter at 6-7; Fidelity Letter at 2.

[79] *See* Data Security Proposal.

[80] SIFMA Letter at 7.

[81] SEC, Order Approving CAT NMS Plan at 715.

[82] *See* Appendix B at 53-54.

[83] Citadel Letter at 8.

cybersecurity requirements—is an advantage of the *ex ante* regulatory regime. By contrast, litigation is an *ex post* approach and therefore, by definition, would react to any security issues. Further, litigation is a lengthy process, unlikely to outpace regulation. This comment also fails to consider that the Participants and FINRA CAT are already required to proactively monitor the CAT's cybersecurity and promptly address any vulnerabilities.[84]

One commenter opined that the Data Security Proposal demonstrates that the Commission no longer believes that "the existing cyber security framework is adequate."[85] The Commission, however, explicitly stated that "CAT Data reported to and retained in the Central Repository is thus subject to what the Commission believes are stringent security policies, procedures, standards and controls."[86] Moreover, as Charles River highlights, the Commission's willingness to propose potential changes—and afford both Industry Members and the Participants a meaningful opportunity to comment on those proposals—highlights the sufficiency and flexibility of the regulatory regime to ensure optimal security of CAT Data.

3) The Commission's Economic Analysis

One commenter opined that Charles River's estimate of "greater than $100 million [in] damage[s]" for certain breach scenarios "may misguide policy makers (sic) into falsely believing the risks may possibly be accepted when it should not."[87] The Participants note that in conducting its own economic analysis of the Participants' then-proposed CAT NMS Plan, the Commission explicitly considered the costs of a potential data breach and concluded that the overall benefits of the CAT outweighed any costs.[88] The Participants also note that when it adopted the Plan and directed the SROs to create the Consolidated Audit Trail in their regulatory capacities, there is nothing to indicate that the Commission contemplated that the Participants could be liable for extensive monetary damages resulting from a data breach or for the costs of protracted litigation with Industry Members.[89]

4) Industry Members' Economic Analysis

SIFMA retained Professor Craig M. Lewis to prepare an economic analysis of the Proposed Amendment.[90] Professor Lewis concludes that the party in control of CAT Data should bear the liability for a data breach and that the risk of a data breach should be addressed by both SEC

---

[84] CAT NMS Plan at 38; 45.

[85] *See* Citadel Letter at 8 (quoting Data Security Proposal at 10).

[86] Data Security Proposal at 10.

[87] Data Boiler Letter at 1 (emphasis omitted).

[88] SEC, Order Approving CAT NMS Plan at 436-47, 704-17; *see also id.* at 620 ("The Commission continues to believe that direct costs in the event of a CAT security breach could be significant, but that certain provisions of Rule 613 and the CAT NMS Plan appear reasonably designed to mitigate the risk of a security breach.").

[89] *See* SEC, Order Approving CAT NMS Plan.

[90] *See* Lewis Report.

regulation and allowing Industry Members to litigate against the Participants.[91] Professor Lewis also opines that CAT LLC is in a better position than Industry Members to insure against potential losses resulting from a data breach.[92]

The Participants disagree with the conclusions in Professor Lewis's report, and have asked Charles River to respond to the issues raised in his analysis. As an initial observation, the Participants note that the Lewis Report appears to advocate for CAT LLC to be held strictly liable for *all* costs associated with *any* CAT Data breach, regardless of the facts and circumstances.[93] However, the Lewis Report provides no economic analysis as to why the longstanding allocation of liability between the Participants and Industry Members—as memorialized in SRO rules and other regulatory reporting facilities—should not apply here.[94]

The Lewis Report also bases much of its analysis on the premise that "Industry Members may be sued by their customers should [CAT] data be compromised."[95] But that premise is not correct. Industry Members routinely disclaim liability to their underlying customers—a fact that Professor Lewis tellingly fails to mention.[96] It is also worth emphasizing that the Limitation of Liability Provisions do not impact the rights of Industry Members' underlying customers, and any attempts to suggest otherwise are baseless.[97] Moreover, as Charles River's scenario analysis indicated, many potential breach scenarios do not involve customer data.[98] Unlike Charles River, Professor Lewis did not conduct a scenario analysis.

Professor Lewis did not conduct a scenario analysis, yet the Lewis Report asserts that "if a cyber-breach occurred, it is likely to be a single event that affects all Industry Members simultaneously."[99] This is not correct. In fact, most of the eight illustrative scenarios identified by Charles River would likely be directed at one or a small group of Industry Members or retail investors.[100] Based on the false assumption that "no Industry Member is likely to be affected without all Industry Members being similarly affected at the same time,"[101] Professor Lewis

---

[91] *Id.*at 5-9, 14.

[92] *Id.* at 11; *see also* Virtu Letter at 3-4; SIFMA Letter at 8-9.

[93] Lewis Report at 5.

[94] The Participants also note that, unlike Charles River, Professor Lewis does not appear to rely on any academic articles or peer reviewed research in support of his conclusions. *See generally* Lewis Report.

[95] Lewis Report at 7.

[96] *See generally* Lewis Report. Professor Lewis likewise fails to mention that disclaiming liability has not prevented Industry Members from having adequate security.

[97] *See infra* at E(4).

[98] *Compare* Appendix B at 18-32 *with* Lewis Report. The Lewis Report, like the SIFMA Letter, appears to conflate risks related to PII with risks related to transaction data.

[99] Lewis Report at 12.

[100] Appendix B at 32.

[101] Lewis Report at 12.

incorrectly concludes that CAT LLC is in a better position than Individual Members to insure against a cyber breach.

Finally, the Lewis Report challenges the Participants' assertion that CAT LLC has obtained the maximum available insurance coverage for a potential breach.[102] The Participants reiterate that CAT LLC has purchased the highest amount of coverage that the current market will provide. Additionally, the Participants regularly evaluate CAT LLC's insurance and intend to purchase additional coverage to the extent it becomes reasonably available.

E. The Regulatory Nature of the CAT

1) Proposals to Shift Liability to Regulators

One commenter—a trade association that represents certain retail and institutional capital markets firms—suggested that the Commission should bear liability in the event of a CAT Data breach.[103] The Participants disagree and note that shifting liability to the Commission is inconsistent with the fundamental nature of the relationship between regulators and regulated entities. The Participants submit that this misconception also underpins certain Industry Members' assertions that liability should be shifted from Industry Members to the Participants. The same principles that protect the Commission from liability for damages apply with equal force to the Participants where, as here, they are acting to fulfill an important regulatory function in their capacities as self-regulatory organizations—i.e., the requirements of Rule 613 and the CAT NMS Plan.

Several commenters characterize the Proposed Amendment as an attempt to "shift" liability from the Participants to Industry Members.[104] The Participants disagree with this characterization and note that it is Industry Members who are proposing a "shift" from the longstanding allocation of liability between Industry Members and the Participants.[105]

Another commenter opined that it is unfair for Industry Members to assume the potential costs of a hypothetical data breach because they are "being forced by regulation to submit data to the CAT."[106] The Participants note that all parties to the CAT—including Industry Members and the Participants themselves—are acting pursuant to Commission mandate. But, unlike Industry Members, the Participants are also fulfilling a regulatory oversight role, and there is no basis for the Participants to assume liability that is invariably assumed by Industry Members (i.e., in the context of other regulatory reporting facilities).

---

[102] *Id.* at 13; *see also* Citadel Letter at 8.

[103] ASA Letter at 3 ("If such a discussion were to have occurred, it is highly probable that all parties would have agreed to take a position that the liability for any breach of the CAT should be placed on the regulator that mandated its existence by law.").

[104] *See generally* Virtu Letter; SIFMA Letter; ASA Letter at 1; Fidelity Letter at 2; FIA PTG Letter at 1; Raymond James Letter at 2.

[105] *See supra* at B.

[106] Virtu Letter at 3.

2) CAT's Regulatory Function

One commenter appears to suggest that the Participants are operating the CAT in connection with their business activities. That commenter opines that allowing the Participants to "hide[e] behind a regulatory shield" would "encourage [the Participants] to [] make high-risk **business decisions**" and "cement an unfair competitive advantage for [the Participants] over broker-dealers and other market participants, whose **business decisions** are subject to liability."[107]

This comment appears to be based on a misunderstanding of the purpose of the CAT and the Participants' mandate under the CAT NMS Plan. Indeed, Rule 613 tasked the SROs with creating and operating the CAT to achieve a core regulatory function—i.e., to "oversee our securities markets on a consolidated basis—and in so doing, better protect these markets and investors."[108] During Rule 613's adoption, the Commission made clear that the rule imposed regulatory obligations on the Participants.[109] And SIFMA recognized the important regulatory function of the CAT, expressing its "belie[f] that a centralized and comprehensive audit trail would enable the SEC and the securities self-regulatory organizations (SROs) to perform their monitoring, enforcement, and regulatory activities more effectively."[110]

3) Regulatory Immunity

The Participants received two contradictory sets of comments regarding the doctrine of regulatory immunity. As discussed below, regulatory immunity does not preclude the use of contractual limitation of liability provisions. Moreover, the divergent and shifting positions among Industry Members on the applicability of regulatory immunity underscores the need for a contractual limitation of liability.

The first category of comments generally argue that a contractual limitation of liability is unnecessary in light of the doctrine of regulatory immunity. For example, one commenter noted "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."[111] That commenter also suggested that the Participants may be seeking "to avoid liability in circumstances in which they misuse CAT Data while acting in a commercial capacity where they might not otherwise be

---

[107] Citi Letter at 4 (quoting Letter from Daniel Keegan, Citi to Elizabeth Murphy, Secretary, U.S. Securities and Exchange Commission, at 3-4 (Aug. 22, 2012), available at https://www.sec.gov/comments/sr-nasdaq-2012-090/nasdaq2012090-5.pdf) (emphasis added); *see also* SIFMA Letter at 8 (suggesting, without basis, that the Participants intend to use CAT Data "while acting in a commercial capacity").

[108] Chairman Jay Clayton, SEC, Statement on the Status of the Consolidated Audit Trail (Nov. 14, 2017), available at https://www.sec.gov/news/public-statement/statement-status-consolidated-audit-trail-chairman-jay-clayton.

[109] SEC, Consolidated Audit Trail, Release No. 34-67457; File No. S7-11-10, at 4 (Oct. 1, 2012) (noting lack of key information in prior audit trails needed for regulatory oversight) and at 20 (noting that prior to the CAT, SROs and the Commission must use a variety of data sources to fulfill their regulatory obligations), available at https://www.sec.gov/rules/final/2012/34-67457.pdf.

[110] Letter from James McHale, SIFMA to Elizabeth Murphy, Secretary, Securities and Exchange Commission, at 1-2 (Aug. 17, 2010), available at https://www.sec.gov/comments/s7-11-10/s71110-63.pdf.

[111] SIFMA Letter at 8.

entitled to regulatory immunity."[112] Another commenter noted that the Proposed Amendment is "unnecessary" and "superfluous" because the Participants are already immune from liability when they are acting as regulators.[113]

The second category contains comments in which Industry Members opined that the Participants should not receive either regulatory immunity or the protection of a limitation of liability provision. For example, one commenter suggests that because the exchanges have for-profit functions (in addition to their regulatory mandates), CAT LLC, the Participants and FINRA CAT should not be entitled to either contractual or regulatory immunity in connection with the operation of the CAT.[114] Additionally, Professor Lewis concludes that CAT LLC should be "responsible for compensating Industry Members for *any* litigation costs associated with a breach or misuse of CAT Data."[115]

The Participants believe that the Limitation of Liability Provisions are necessary despite their regulatory immunity. Although the Participants firmly believe that they are entitled to regulatory immunity in connection with the operation of the CAT, even litigation in which a court ultimately holds that regulatory immunity applies may result in significant disruption and expense for the Participants, and there is no guarantee that all courts would agree that the Participants' immunity defense extends to the particular claims at issue.

The risk presented by the uncertainty of litigation is magnified by Industry Members' continuously shifting positions regarding the applicability of regulatory immunity. As noted above, certain Industry Members agree that regulatory immunity should apply to the Participants in connection with the CAT; others advocate for an unqualified right to litigate against the Participants for damages. Notably, SIFMA has challenged SRO immunity generally and specifically with respect to the CAT; yet SIFMA conveniently invokes regulatory immunity in its comment letter to argue that the Limitation of Liability Provisions are unnecessary because regulatory immunity should protect the Participants from liability in connection with the CAT.[116] But, in connection with CAT reporting, SIFMA *previously* asked the Commission to:

- "direct the SROs to amend the CAT NMS Plan (or amend the CAT NMS Plan itself) to waive regulatory immunity for data breach claims, thereby allowing broker-dealers or customers to seek indemnification or pursue a lawsuit against the SROs"; and

---

[112] *Id.*

[113] Citadel Letter at 3-4.

[114] *See* Citi Letter at 2-4.

[115] Lewis Report at 5 (emphasis added).

[116] SIFMA's belated concession that regulatory immunity should protect the Participants from liability in connection with the CAT is undermined by its repeated assertion that the party who possesses the data should bear all risk associated with a data breach. *Compare* SIFMA Letter at 8 *with* SIFMA Letter at 4-5. Further, if immunity applies, the Limitation of Liability Provisions do not substantively impact Industry Members rights in relation to the SROs.

- "direct FINRA CAT not to assert regulatory immunity for data breach claims arising out of FINRA CAT's role as the CAT Plan Processor or amend the CAT NMS Plan to include such a provision."[117]

More broadly, SIFMA's longstanding position is that Congress should abrogate regulatory immunity by statute.[118] And notwithstanding SIFMA's ambiguous position regarding the applicability of regulatory immunity to the CAT, individual SIFMA members have made clear that they do not believe that the Participants should be entitled to regulatory immunity in connection with CAT Data.[119] The uncertainty regarding how courts will apply regulatory immunity, coupled with Industry Members' inconsistent positions and efforts to abolish regulatory immunity legislatively, necessitate a contractual limitation of liability to protect the Participants in connection with the operation of the CAT.

Finally, even if a court determines that the Participants, CAT LLC and FINRA CAT are entitled to regulatory immunity, CAT LLC could still face substantial legal fees and expenses—which ultimately will be passed along to Industry Members as part of CAT LLC's joint funding, and then further to retail investors—defending against meritless claims prior to a judicial determination that the doctrine applies.[120] The Limitation of Liability Provisions would appropriately deter such lawsuits and allow the Participants and the Commission to focus on the shared goal of implementing the CAT NMS Plan as quickly, efficiently, and securely as possible. For those reasons (and in light of the uncertainty discussed above), the Commission has repeatedly approved contractually based limitations of liability even where: 1) the SROs are acting pursuant to their regulatory duties, 2) in performance of a federally mandated obligation, 3) that would otherwise be performed by the SEC.[121] Because the Participants are implementing CAT at the behest of the SEC to create a regulatory tool for the Commission and SROs, they are acting in the place of the

---

[117] Letter from Kenneth Bentsen, SIFMA to the Honorable Jay Clayton, Chairman, U.S. Securities & Exchange Commission, at 3 (Nov. 11, 2019), available at https://www.sifma.org/wp-content/uploads/2020/01/SIFMA-Letter-to-SEC-Chairman-Clayton-on-CAT-Liability-and-Access-Issues-November-11-2019.pdf.

[118] *See, e.g.*, Letter from Theodore Lazo to Chair Mary Jo White, U.S. Securities and Exchange Commission, at 8 (July 31, 2013), available at https://www.sifma.org/wp-content/uploads/2017/05/sifma-submits-comments-to-the-sec-requesting-a-review-of-the-self-regulatory-structure-of-securities-markets.pdf (noting SIFMA's goal of seeking "an eventual legislative end to" regulatory immunity for SROs).

[119] *See* Citi Letter at 2-4.

[120] *See* Appendix B at 44-47 (discussing the negative impact on social welfare of costs associated with CAT LLC defending against litigation regarding a data breach).

[121] *See* Proposed Amendment at n.14-15, 21. The Participants categorically reject the baseless implication in certain comment letters that the Participants intend to use CAT Data for commercial purposes. *See* SIFMA Letter at 8; Citadel Letter at 4. These commenters fail to point out that commercial use of CAT Data is prohibited both by the CAT NMS Plan as well as the Reporter Agreement. *See* CAT Reporter Agreement, Section 2.1, available at https://www.catnmsplan.com/sites/default/files/2020-05/Consolidated-Audit-Trail-Reporter-Agreement-amended_0.pdf ("CAT Reporter and CATLLC acknowledge that CATLLC, the Participants, and the Plan Processor are not authorized by the CAT NMS Plan to use the submitted CAT Data for commercial purposes, provided that a Participant which is a CAT Reporter may use its own submitted Raw Data for such purposes.").

SEC to discharge a federal mandate and should receive contractual protections in connection with the discharge of their regulatory duties.

At bottom, if the Commission agrees with the position of the Participants (and certain Industry Members) that the Participants, CAT LLC, and FINRA CAT should not be liable for monetary damages while acting to fulfill an important regulatory function in their capacities as self-regulatory organizations, the Commission's sole mechanism for ensuring that protection is to endorse the contractual Limitation of Liability Provisions. The Commission should approve the Proposed Amendment.

4) Scope of the Proposed Amendment and SEC Oversight

Several commenters misstate the scope of the Proposed Amendment and its impact on the potential liability of CAT LLC, the Participants, and FINRA CAT. For example, one commenter claims that if the Commission approves the Proposed Amendment, the Participants would have "no potential for penalty either fiscal or reputational."[122] Another commenter characterizes the Proposed Amendment as an effort by the Participants to "extinguish their liability" in the event of a data breach.[123]

These comments are based on a misunderstanding of the scope of the Limitation of Liability Provisions. The Proposed Amendment does not extinguish liability; rather, it addresses the question of whether the historical allocation *between Industry Members and the Participants* should apply to CAT Data (that the Participants are collecting pursuant to a regulatory mandate) and be memorialized in the CAT Reporter Agreement and Reporting Agent Agreement.

The Proposed Amendment does not impact the rights or obligations of third parties, including Industry Members' customers. The Proposed Amendment also does not impact the broad regulatory oversight that the Commission exercises over the CAT via the agency's examination and enforcement functions.[124] FINRA CAT's and the Participants' cybersecurity policies, procedures, systems, and controls are subject to examination by the Division of Examinations (on both a for-cause and cyclical basis).[125] And contrary to the position of certain commenters that the SROs seek to disclaim *all* liability, any cybersecurity-related violations (e.g., failure to comply

[122] Citi Letter at 2.

[123] SIFMA Letter at 9.

[124] One commenter suggested that the Proposed Amendment would protect a Participant from all liability even if that Participant violated the CAT NMS Plan by using CAT Data for non-regulatory purposes. *See* Citadel Letter at 4-5. However, regulatory immunity applies to private litigation—not SEC regulation or enforcement. The Proposed Amendment would not curtail the Commission's "formidable oversight power to supervise, investigate, and discipline" a Participant "for any possible wrongdoing or regulatory missteps," regardless of whether the Participants are generally afforded regulatory immunity and/or contractual limitations of liability in connection with the operation of the CAT. *In re NYSE Specialists Sec. Litig.*, 503 F.3d 89, 101-02 (2d Cir. 2007) (Sotomayor, J.) (discussing "manifold" alternatives to private suits for reviewing SRO conduct). Any assertion that the Limitation of Liability Provisions could curtail the Commission's enforcement power is baseless.

[125] Appendix B at 43.

with Regulation SCI) could, of course, be referred to the Division of Enforcement for an investigation and potential enforcement action.[126]

Considering the importance of the CAT to the Commission's mission of protecting investors and maintaining fair, orderly, and efficient markets, the Participants expect that the Commission will utilize its examination and enforcement authority as appropriate. Since the adoption of Rule 613 of Regulation NMS, the Consolidated Audit Trail has been a significant regulatory priority to enhance the SEC's and the SROs' tools to "oversee our securities markets on a consolidated basis—and in so doing, better protect these markets and investors."[127] In recognition of the importance of the CAT to the National Market System, the Commission and its Division of Trading and Markets have taken an active oversight role including by participating in all committees and working groups, hosting weekly update meetings, proactively proposing amendments to the CAT NMS Plan, and examining FINRA CAT's policies, procedures, systems, and controls. Data security has been of particular importance, and the Commission has recently reiterated that "[t]he security and confidentiality of CAT Data has been—and continues to be—a top priority of the Commission."[128]

Tellingly, no commenters have offered any explanation as to why the SEC's regulatory regime—which includes cybersecurity protocols developed and refined based on feedback from Industry Members—is insufficient to ensure adequate cybersecurity for CAT Data, or what deficiencies in the Commission's oversight necessitate that Industry Members be afforded an unprecedented private right of action against their regulators.[129] Commenters' opposition to the Proposed Amendment thus amounts, at bottom, to an unsubstantiated challenge to the adequacy of the Commission's CAT oversight.

F. Constitutionality of Collecting CAT Data

One commenter raised concerns regarding what it perceives to be "massive government surveillance" and the "Fourth Amendment right to be free of unwarranted search or seizure."[130] That commenter advocates that the Commission should require that a search warrant be obtained, or, at a minimum, that "symptoms of irregularity … are substantiated" before the Commission or

---

[126] Appendix B at 3, 37. As Charles River notes, unlike Industry Members, "[t]he SEC … is uniquely positioned to consider the costs and benefits of taking enforcement action, and to tailor the scope and nature of enforcement proceedings in a way that best balances the competing stakeholder and public interests the CAT is designed to serve." *Id.* at 37.

[127] Chairman Jay Clayton, SEC, Statement on the Status of the Consolidated Audit Trail.

[128] Data Security Proposal at 9.

[129] The Participants also disagree with commenters' assertions that the Limitation of Liability Provisions would somehow shield the Participants and FINRA CAT from reputational harm. *See* Citi Letter at 2. Charles River's analysis specifically highlights the role of reputational harm as one factor—among many (including SEC oversight)—that incentivizes the Participants to take appropriate cybersecurity precautions and underscores the conclusion that allowing Industry Members to sue their regulators for damages increases costs without any benefit. *See, e.g.*, Appendix B at 12.

[130] Data Boiler Letter at 2 (emphasis omitted).

the Participants can utilize CAT Data.[131] This comment is beyond the scope of the Proposed Amendment, which relates solely to the allocation of liability in the event of a CAT Data breach. The Participants also note that the CAT NMS Plan governs the permissible use of CAT Data, and that the Participants intend to fully comply with the Plan.

G. Potential Mechanisms to Compensate Injured Parties

One commenter noted that the *ex-ante* regulatory approach to mitigating the potential risk of a CAT Data breach does not provide an inherent mechanism to compensate Industry Members harmed by a potential cyber incident.[132] The Participants acknowledge that, as Charles River explained, the regulatory regime is generally silent with respect to the most efficient method to compensate injured parties.[133] Charles River acknowledged this economic reality and offered several suggestions to cover potential losses including insurance, industry loss warranties, and catastrophe bonds.[134] The Participants have been—and remain—willing to discuss any of these compensation mechanisms with Industry Members. The Participants would also welcome a discussion with the Commission to address the viability of these mechanisms and how they might be funded.

One commenter notes that "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… ."[135] But as the Participants have already made clear, CAT LLC has obtained the maximum extent of cyber-breach insurance coverage available under current market conditions.[136]

Another commenter opines that "[i]f the Proposal is approved, CAT LLC would have no incentive to pursue more robust insurance protection because it would have no litigation exposure."[137] The Participants disagree and note that at the time CAT LLC decided to purchase the maximum available insurance, the then-draft Reporter Agreement contained a broad limitation of liability provision (which was ultimately executed by all but approximately 60 Industry Members). That history makes clear that the Participants' decision to purchase the maximum coverage available is not contingent on whether they are protected by a limitation of liability provision.

One commenter suggested that "Industry Members should be added as 'additional insured parties' under CAT LLC's" insurance policies.[138] Another commenter echoed Charles River's suggestion that "other financial tools [such as] industry loss warranties or catastrophe bonds could be used to

---

[131] *See id*. (emphasis omitted).

[132] SIFMA Letter at 10.

[133] Appendix B at 50.

[134] Appendix B at 50-53.

[135] SIFMA Letter at 10-11.

[136] *See* Proposed Amendment at 10.

[137] SIFMA Letter at 10.

[138] Virtu Letter at 3.

supplement traditional insurance."[139] The Participants have repeatedly expressed their willingness to consider any proposals offered by Industry Members to compensate parties harmed by a potential CAT Data breach, and look forward to further engaging with Industry Members and the Commission regarding specific suggestions raised during the comment process. The Participants note, however, that creating mechanisms to compensate Industry Members in the event of a data breach does not obviate the need for the Limitation of Liability Provisions.

Finally, as discussed above, as part of the Commission's regulatory oversight of CAT LLC, the Participants, and FINRA CAT, the Commission is empowered to bring enforcement actions for violations of its cybersecurity requirements.[140] As Congress recently made clear, the Commission's enforcement authority includes the ability to order individuals and entities that violate the securities laws to disgorge ill-gotten gains. The Commission may use those funds (as well as any civil monetary penalties imposed) to compensate harmed parties.[141] The Participants note that if the Commission determines Industry Members were harmed due to cybersecurity violations in connection with CAT Data, any disgorgement and civil monetary penalties collected could be used to compensate victims of a potential breach.[142]

---

[139] SIFMA Letter at 10.

[140] *See generally supra*.

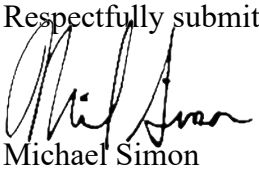
[141] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, H.R. 6395, 116th Cong. § 6501(a)(1) (2021) (enacted), available at https://www.congress.gov/bill/116th-congress/house-bill/6395.

[142] *See* 17 CFR 201.1100, available at https://www.govinfo.gov/content/pkg/CFR-2014-title17-vol3/pdf/CFR-2014-title17-vol3-sec201-1100.pdf ("In any agency process initiated by an order instituting proceedings in which the Commission or the hearing officer issues an order requiring the payment of disgorgement by a respondent and also assessing a civil money penalty against that respondent, the Commission or the hearing officer may order that the amount of disgorgement and of the civil penalty, together with any funds received pursuant to 15 U.S.C. 7246(b), be used to create a fund for the benefit of investors who were harmed by the violation.").

* * * * *

Thank you for your attention to this matter. Please contact me at [redacted] if you have any questions or comments.

Respectfully submitted,



Michael Simon
CAT NMS Plan Operating Committee Chair

cc: The Hon. Allison Herren Lee, Acting Chair
The Hon. Caroline A. Crenshaw, Commissioner
The Hon. Hester M. Peirce, Commissioner
The Hon. Elad L. Roisman, Commissioner
Mr. Hugh Beck, Senior Policy Advisor, Regulatory Reporting to Acting Chair Lee
Mr. Christian Sabella, Acting Director, Division of Trading and Markets
Mr. David S. Shillman, Associate Director, Division of Trading and Markets
Mr. David Hsu, Assistant Director, Division of Trading and Markets
Mr. Mark Donohue, Senior Policy Advisor, Division of Trading and Markets
Ms. Erika Berg, Special Counsel, Division of Trading and Markets
CAT NMS Plan Participants