May 18, 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"),[4] the Participants[5] 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 Proposed Amendment was accompanied by an economic analysis conducted by Charles River Associates

---

[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] Letter from Michael Simon, CAT NMS Plan Operating Committee Chair to Vanessa Countryman, Secretary, Securities and Exchange Commission (Dec. 18, 2020) (the "Proposed Amendment"), available at https://www.catnmsplan.com/sites/default/files/2020-12/12.18.2020-Proposed-Amendment-to-the-CAT-NMS-Plan.pdf.

[5] 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.

("Charles River"), which was memorialized in Appendix B to the Proposed Amendment ("Appendix B").

### A. Initial Comments Regarding the Proposed Amendment and the Commission's Order Instituting Proceedings

The SEC received eleven comment letters in response to the Proposed Amendment, and the Participants responded to those comments on April 1, 2021 (the "Response Letter").[6] Additionally, on April 5, 2021, Charles River filed a report (the "CRA Reply")[7] that: 1) responded to an economic analysis conducted by Professor Craig M. Lewis of Vanderbilt University and 2) addressed economic issues implicated by comments from industry members ("Industry Members") and the Securities Industry and Financial Markets Association ("SIFMA").

On April 6, 2021, the Commission issued an Order Instituting Proceedings to Determine Whether to Approve or Disapprove an Amendment to the National Market System Plan Governing the Consolidated Audit Trail (the "OIP") pursuant to Rule 608(b)(2)(i) of Regulation NMS.[8] The OIP requested additional comments regarding: a) the impact of the Limitation of Liability Provisions on the incentives of the Participants to ensure the security of the CAT and CAT Data; b) any regulatory immunity applicable to the Participants; and c) the application of the Limitation of Liability Provisions to willful misconduct, gross negligence, bad faith, or criminal acts.[9] The Commission also requested comments regarding the impact of the Proposed Amendment on efficiency, competition, and capital formation, and regarding whether any modifications to the Proposed Amendment were appropriate and consistent with the Exchange Act.[10]

### B. Overview of Comment Letters and Summary of the Participants' Responses

The Commission received two comment letters—from SIFMA and Data Boiler Technologies, LLC ("Data Boiler")—in response to the OIP.[11] In general, SIFMA reiterates its objection to the

---

[6] Letter from Michael Simon, CAT NMS Plan Operating Committee Chair to Vanessa Countryman, Secretary, Securities and Exchange Commission, (Apr. 1, 2021), available at https://www.sec.gov/comments/4-698/4698-8573527-230862.pdf.

[7] Craig M. Lewis, Ph.D., CRA Response to: Economic Analysis of Proposed Amendment to National Market System Plan Governing the Consolidated Audit Trail (Apr. 5, 2021), available at https://www.sec.gov/comments/4-698/4698-8634778-230925.pdf.

[8] *See* Release No. 34-391487; File No. 4-698 (Apr. 6, 2021), available at https://www.sec.gov/rules/sro/nms/2021/34-91487.pdf, 86 Fed. Reg. 19054 (Apr. 12, 2021), available at https://www.govinfo.gov/content/pkg/FR-2021-04-12/pdf/2021-07390.pdf; 17 C.F.R. § 242.608(b)(2)(i).

[9] OIP at 26-27.

[10] *Id.* at 27.

[11] Letter from Ellen Greene, SIFMA to Vanessa Countryman, Secretary, U.S. Securities and Exchange Commission (May 3, 2021) (the "SIFMA Letter"), available at https://www.sec.gov/comments/4-698/4698-8751243-237404.pdf; Letter from Kelvin To, Data Boiler Technologies, LLC to Vanessa Countryman, Secretary, U.S. Securities and Exchange Commission (May 3, 2021) (the "Data Boiler Letter"), available at https://www.sec.gov/comments/4-698/4698-8749987-237362.pdf. The comments in the Data Boiler Letter are largely unrelated to the Proposed Amendment and the specific issues highlighted by the Commission in the OIP. For example, the letter discusses public policy concerns regarding "Massive Government Surveillance" and raises

Proposed Amendment and argues that Industry Members should be permitted to litigate against the self-regulatory organizations ("SROs") for monetary damages because the Commission's regulatory regime does not create sufficient incentives for the Participants to adequately protect CAT Data.[12] SIFMA also argues that a contractual limitation of liability is unnecessary in light of regulatory immunity—yet, SIFMA does not indicate that it and its constituent Industry Members will abandon their extensive efforts to challenge the doctrine in court or cease lobbying Congress to abrogate it by statute.[13]

Alternatively, SIFMA suggests that if the Commission approves the Proposed Amendment, it should modify the Limitation of Liability Provisions to exclude willful misconduct, gross negligence, bad faith, and criminal acts.[14] In that regard, the SIFMA Letter notes that on the same day on which it filed its comment letter in response to the OIP, SIFMA provided the Participants with a proposal to revise the Limitation of Liability Provisions to exclude willful misconduct, gross negligence, bad faith, and criminal acts, and limit liability only when the Participants are acting "solely" in their regulatory capacities.[15] The SIFMA Letter acknowledges that the SIFMA term sheet is a response to a settlement proposal that the Participants provided to SIFMA fourteen months ago.[16]

After reviewing the comments that the Commission received in response to the OIP, the Participants maintain that the Proposed Amendment is consistent with the Exchange Act. The Commission's regulatory regime—backed by its examination and enforcement functions—provides powerful incentives for the Participants, CAT LLC, and FINRA CAT to take adequate cybersecurity precautions. No commenter has demonstrated (either in response to the OIP or the Proposed Amendment) that the SEC lacks the ability to adequately regulate the CAT and the Participants. Nor has any commenter explained how the prospect of Industry Member litigation would increase the Participants' and FINRA CAT's incentives to protect CAT Data. For those reasons (among others), adding the prospect of Industry Member litigation to the Commission's existing regulatory regime would not result in any meaningful benefit to the CAT's cybersecurity.

By contrast, the prospect of Industry Member litigation undoubtedly would result in substantial additional costs. As demonstrated by Charles River's extensive economic analysis, the costs of litigating a potential CAT Data breach are likely to be both substantial and unquantifiable on an

---

arguments under the Fourth Amendment to the U.S. Constitution against the collection and storage of CAT Data. *See* Data Boiler Letter at 1, 5, 10. The letter also raises various comments regarding the proposed funding model for the CAT, which is also beyond the scope of the Proposed Amendment. *See id.* at 5-9. To the extent that certain comments in the Data Boiler Letter are relevant to the Proposed Amendment, the Participants address them below.

[12] Although Professor Lewis submitted a report in response to the Proposed Amendment, SIFMA did not file a report from Professor Lewis to respond to the OIP or to the issues raised in the CRA Reply.

[13] SIFMA Letter at 6-7.

[14] *Id*. at 7-9.

[15] *Id*. at 11.

[16] *Id*. at 10-11.

*ex-ante* basis.[17] There is simply no precedent for Industry Members' extraordinary demand that their regulators bear liability that includes hypothetical "black swan" cyber breaches. And even in the absence of actual litigation regarding a breach, shifting potential liability from Industry Members to the Participants would create additional costs and distract the Participants from the vital regulatory mission vested in them by the Exchange Act. Critically, many of these added costs—whether resulting from litigation or any other source—ultimately would be passed along to investors.

Moreover, contrary to SIFMA's assertion, the Participants' regulatory immunity does not obviate the need for the Limitation of Liability Provisions. Although the Participants firmly believe that they are entitled to regulatory immunity in connection with their operation of the CAT, there is no guarantee that all courts will agree that the Participants' immunity extends to the claims at issue. The uncertainty inherent in litigation is compounded here by SIFMA's legislative and judicial challenges to the immunity doctrine—both generally and specifically in relation to CAT Reporting. Indeed, while SIFMA now insists that the Participants should rely on regulatory immunity in connection with the CAT (despite SIFMA asking the Commission to amend the CAT NMS Plan to prohibit the Participants from asserting immunity defenses), SIFMA has made no representations that Industry Members will refrain from challenging SRO immunity in potential future litigation regarding CAT Data. In any event, any such representation would not be credible, as SIFMA's expressly stated goals include "an eventual legislative end" to SRO immunity.[18] For those reasons, the Participants have historically sought and received contractually-based liability protections from Industry Members—even where the Participants also have strong immunity defenses. These contractual protections that have long governed the relationships between SROs and Industry Members should plainly apply to CAT Reporting.

Finally, the limitations of liability between the Participants and Industry Members do not typically exclude gross negligence, willful misconduct, bad faith, or criminal acts. SIFMA's proposal to exclude these items from the Limitation of Liability Provisions is generally inconsistent with the liability provisions of other NMS plans, regulatory reporting facilities, and SRO rules. The historical absence of such exclusions from provisions that limit liability of regulators to the entities they regulate is good policy and consistent with the Exchange Act. If the Commission creates exclusions to the Limitation of Liability Provisions in the Reporter Agreement, any future CAT Data breach inevitably will lead to litigation in which putative plaintiffs (and their counsel) attempt to demonstrate that those exclusions apply, regardless of the facts surrounding the breach. Adding substantive exclusions to the Limitation of Liability Provisions would thus frustrate a primary purpose of a contractual limitation—i.e., avoiding the costs associated with defending meritless lawsuits and enabling regulators to focus on their regulatory mandates.

---

[17] Appendix B at 46.

[18] *See* Response Letter at 24 n.118 (citing Letter from Theodore Lazo, SIFMA 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.).

For those reasons, and as discussed in detail below, the Participants respectfully request that the Commission approve the Proposed Amendment without modifying the Limitation of Liability Provisions.

### C. Incentives to Ensure the Security of the CAT and Other Economic Issues

#### 1) Economic Analysis of Incentives

SIFMA asserts that "the threat of litigation" is necessary to create incentives for the Participants to take appropriate cybersecurity measures to safeguard CAT Data.[19] SIFMA's conclusory assertion is not accompanied by any explanation as to why the current incentives are inadequate.[20] As discussed below, the Commission's regulatory enforcement regime fully incentivizes the Participants to create and maintain effective cybersecurity policies, procedures, systems, and controls.

As an initial matter, the SIFMA Letter generally ignores the various factors that inform the Participants' incentives to protect CAT Data.[21] Instead, SIFMA mostly reiterates its arguments in support of certain cybersecurity measures discussed in the Commission's August 21, 2020 CAT Data Security Proposal (the "Data Security Proposal").[22] SIFMA also notes that it has requested "over the years" that Industry Members should be added to the Operating Committee and the CAT Security Working Group.[23] These considerations are largely irrelevant to the central question posed by the Commission's OIP—namely, whether the Participants, CAT LLC, and FINRA CAT are appropriately incentivized to protect CAT Data. The SIFMA Letter is generally silent on that point and fails to discuss the various factors that Charles River has highlighted as creating strong incentives for the Participants, CAT LLC, and FINRA CAT to implement appropriate cybersecurity precautions, including:

- the Commission's regulatory enforcement regime with the Commission's attendant powers to impose civil monetary penalties, disgorgement of ill-gotten gains, industry suspensions and bars, and revocation of an exchange's registration (among other relief);
- the severe reputational harm that would result to the Participants and FINRA CAT in the event of a CAT Data breach;
- the financial and reputational harm that could result to Amazon Web Services (the primary technology infrastructure provider to CAT LLC) in the event of a CAT Data breach;

---

[19] *See* SIFMA Letter at 6 and *generally*.

[20] *Id.*; *see also* CRA Reply at 4.

[21] *See* SIFMA Letter at 4-6, Section II(A).

[22] *See id*. at 6; 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), 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.

[23] SIFMA Letter at 6.

- relationships between CAT LLC and its various technology vendors, many of which can suggest specific cybersecurity proposals based on their specialized knowledge and unique access to CAT operations;
- CAT LLC's incentives to satisfy insurance underwriting standards and to lower insurance premiums; and
- incentives created by the fact that a data breach could compromise the Participants' ability to use CAT Data to carry out the regulatory mandates vested in them by the Exchange Act as SROs.[24]

Finally, the Participants note that although the exchanges are protected by both regulatory immunity and Commission-approved liability limitations in connection with the operation of their own systems, the Participants take extensive measures to safeguard data in their possession. This reality demonstrates that the Participants are fully incentivized to maintain appropriate cybersecurity measures even without the prospect of Industry Member litigation.

In the multiple rounds of comments that the Commission has provided to date, commenters have not advanced any cogent argument to undermine the Participants' position that the Participants, CAT LLC, and FINRA CAT are already appropriately incentivized to adopt all necessary cybersecurity measures to protect CAT Data.

2) The Commission's Regulatory Regime

In the Response Letter, the Participants observed that "Commenters' opposition to the Proposed Amendment thus amounts, at bottom, to an unsubstantiated challenge to the adequacy of the Commission's CAT oversight," including the Commission's broad and sweeping authority to regulate the CAT and the Participants.[25] The SIFMA Letter characterizes this observation as "absurd;"[26] yet, in the very next paragraph, SIFMA claims that, if the Commission adopts the Proposed Amendment, the Participants would "**completely avoid[] responsibility** … for the consequences of any breach."[27] If, as SIFMA claims, the SROs can "completely avoid[] responsibility" for a breach, it logically follows that SIFMA does, in fact, believe that the Commission's oversight is inadequate.

There is, however, no serious dispute that the Commission has broad enforcement powers, including the authority to seek various forms of monetary and non-monetary relief against the SROs and their representatives.[28] Because they are subject to stringent SEC oversight, CAT LLC, the Participants, and FINRA CAT are highly incentivized to comply with the Commission's mandates and minimize the likelihood of an enforcement action. Additionally, FINRA CAT's and the Participants' cybersecurity policies, procedures, systems, and controls are subject to

---

[24] *See* Appendix B at 19, 42-44, 53-54; CRA Reply at 3-4.

[25] Response Letter at 25-26, Section E(4).

[26] *See* SIFMA Letter at 4.

[27] *See id*. at 5 (emphasis added).

[28] *See generally* Exchange Act, 15 U.S.C. § 78a.

examination by the Division of Examinations (on both a for-cause and cyclical basis).[29] Accordingly, the Participants are highly motivated to take all measures to avoid the Division of Examinations issuing a deficiency letter or an enforcement referral.

It comes as no surprise that courts have recognized that the Commission's regulatory regime creates strong incentives for the SROs to comply with the SEC's mandates. As the Second Circuit explained in concluding that "alternatives to damage suits against [an SRO] … are manifold," "[t]he SEC, after all, retains formidable oversight power to supervise, investigate, and discipline [an SRO] for any possible wrongdoing or regulatory missteps."[30] In elaborating on the SEC's oversight abilities, the Second Circuit highlighted that the Commission's enforcement action against the exchange at issue: 1) imposed substantial civil monetary penalties, 2) required the exchange to implement new methods of regulation and oversight, and 3) garnered widespread public attention.[31] Notably, the characteristics that the Second Circuit highlighted are attributes of *ex ante* regulatory regimes that, as Charles River has explained, properly incentivize entities to take appropriate precautions—and thereby render *ex post* litigation (of the sort for which SIFMA advocates here) an unnecessary cost.[32]

3) The Pace of the Regulatory Regime and Emerging Cyber Threats

SIFMA asserts that the Proposed Amendment is inappropriate because the regulatory process might not keep pace with emerging and evolving cyber threats.[33] This comment fails to consider that the Commission's regulatory regime has a mechanism designed to address this concern. Indeed, the CAT NMS Plan requires that the Participants and FINRA CAT proactively monitor the CAT's cybersecurity and promptly address any vulnerabilities, even in the absence of an explicit Commission mandate to do so.[34] SIFMA's contention that litigation is "necessary" to ensure that the Participants proactively adapt the CAT's cybersecurity once again fails to give appropriate recognition to the Commission's regulatory requirements and oversight.[35]

---

[29] Appendix B at 43.

[30] *In re NYSE Specialists Sec. Litig.*, 503 F.3d 89, 101 (2d Cir. 2007) (citations omitted); *see also DL Capital Grp., LLC v. Nasdaq Stock Mkt., Inc.,* 409 F.3d 93, 95 (2d Cir. 2005) ("[I]f an SRO has violated, or is unable to comply with, *inter alia*, the provisions of the Exchange Act, its own rules, or the rules of the SEC, the SEC is authorized to suspend or even revoke an SRO's registration, as well as to impose lesser sanctions.") (citing 15 U.S.C. § 78s(g)).

[31] *In re NYSE Specialists*, 503 F.3d at 102.

[32] *See* Appendix B at 34-38, 53-54.

[33] *See* SIFMA Letter at 5-6.

[34] *See* CAT NMS Plan at 38, 45. The CAT NMS Plan also requires that FINRA CAT's Chief Information Security Officer monitor potential emerging and evolving cybersecurity threats. Moreover, such threats are also a priority of CAT's Security Working Group, which meets regularly to ensure that FINRA CAT and the Participants are complying with best practices. The combined efforts, mandates, and expertise of the Security Working Group, FINRA CAT's and the Participants' Chief Information Security Officers, and the Commission provide for a system well-equipped to keep pace with emerging threats to CAT Data.

[35] *See* SIFMA Letter at 6.

SIFMA's comment is also based on a misunderstanding of the relevant economic principles. As Charles River explains, the deliberate nature of the process for considering new proposed cybersecurity measures—which affords all constituencies (including Industry Members) the opportunity to provide feedback and allows the Commission (including its Chief Information Security Officer) to be the ultimate arbiter of cybersecurity requirements—is an advantage of the *ex ante* regulatory regime. By contrast, litigation would require the Commission to share that responsibility with the courts, whose rulings could diverge from each other and diverge from or even conflict with the Commission's positions on cybersecurity.[36] Further, litigation is a lengthy process, unlikely to outpace regulation.

Additionally, SIFMA's comment incorrectly assumes that the Commission may only utilize the formal rule-making process to address emerging cyber threats. To the contrary, the Commission and its staff have multiple tools at their disposal to motivate regulated entities—like the Participants—to expeditiously modify their cybersecurity regimes. For example, the Division of Examinations, which has prioritized cybersecurity issues, often releases risk alerts in response to emerging concerns.[37] Although the substance of those alerts is often characterized as "best practices," regulated entities take such guidance seriously and react accordingly.

4) August 2020 CAT Data Security Proposal

SIFMA argues that the mere fact that some Participants raised issues with the Data Security Proposal suggests that the Participants are not adequately incentivized to protect CAT Data.[38] According to SIFMA, it is "absurd" that certain Participants oppose specific elements of the proposal while also seeking the protection of the Limitation of Liability Provisions.[39] The Participants disagree.

---

[36] As discussed in the Proposed Amendment, 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. *See* Response Letter at 18-19, Section D(2).

[37] *See, e.g.*, Office of Compliance Inspections and Examinations, Risk Alert: Safeguarding Customer Records and Information in Network Storage – Use of Third Party Security Features (May 23, 2019), available at https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Network%20Storage.pdf; Office of Compliance Inspections and Examinations, National Exam Program Risk Alert: Observations from Investment Adviser Examinations Relating to Electronic Messaging (Dec. 14, 2018), available at https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Electronic%20Messaging.pdf; Office of Compliance Inspections and Examinations, Risk Alert: Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P—Privacy Notices and Safeguard Policies (Apr. 16, 2019), available at https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf.

[38] *See* SIFMA Letter at 5. As the Participants noted in their collective comment letter on the Data Security Proposal, the collective letter represented the consensus of the Participants but individual Participants reserved the right to submit their own views on the Proposal, which a number of Participants did.

[39] *See id*. at 5.

The Participants' issues with the Data Security Proposal were informed by their belief that the Commission's proposal will "hamper the Participants' ability to perform their self-regulatory responsibilities" and create "additional security issues for the CAT" (including by impeding the Participants' and FINRA CAT's ability to rapidly adapt to emerging cybersecurity threats), and is therefore ultimately not justifiable based on a cost-benefit analysis.[40] Far from supporting SIFMA's argument that the Participants are not properly incentivized to take appropriate cybersecurity measures, the Participants' comments on the Data Security Proposal indicate that they are keenly focused on whether any proposed modifications to the CAT will enhance cybersecurity and facilitate the SROs' vital regulatory mission. Further, the Participants did not object to the entire Data Security Proposal, and, indeed, the component of the proposal that relates to the exclusion of PII, for example, is already on track to be implemented. At bottom, SIFMA mischaracterizes comments regarding whether the Commission's proposal will improve the CAT's cybersecurity as evidence that the Participants are not properly incentivized.

Additionally, as discussed in the Response Letter, under the Commission's regulatory regime, all interested parties—including CAT LLC, the Participants, and Industry Members—provide feedback to the Commission regarding any proposals involving 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"[41]—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 from Industry Members would not provide any meaningful additional benefits to the CAT's cybersecurity.[42]

5) Industry Member Input Regarding the CAT's Cybersecurity

SIFMA contends that the Commission's regulatory regime has not provided Industry Members with sufficient opportunities to provide feedback regarding the CAT's cybersecurity.[43] SIFMA also reiterates arguments that Industry Members should be added to CAT's Operating Committee and the CAT Security Working Group.[44]

Industry Members, in fact, have ample opportunities to contribute their perspectives regarding the CAT's cybersecurity. For a detailed discussion regarding the extensive input that Industry

---

[40] Letter from Michael Simon, CAT NMS Plan Operating Committee Chair to Vanessa Countryman, Secretary, Securities and Exchange Commission, at 1-2 (Dec. 4, 2020) (the "CAT Comment Letter on Data Security Proposal"), available at https://www.sec.gov/comments/s7-10-20/s71020-8100247-226195.pdf.

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

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

[43] SIFMA Letter at 6.

[44] *Id.*

Members have concerning the CAT's cybersecurity, please see Section C(4) of the Response Letter.[45]

Data Boiler proposed 26 cyber "security and privacy clauses" for the Participants' and the Commission's consideration.[46] That proposal, which was copied verbatim from Data Boiler's submissions in response to the Data Security Proposal as well as its comment letter regarding the Proposed Amendment, is beyond the scope of the Proposed Amendment, which relates solely to the allocation of liability in the event of a CAT Data breach.[47]

The Participants reiterate 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."[48] 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 CAT's security and consider whether and how it can be enhanced on an ongoing basis.[49] 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) to determine the CAT's required security measures in a manner consistent with the Exchange Act and other applicable statutes, rules, and regulations.[50]

---

[45] Response Letter at 13-15, Section C(4).

[46] Data Boiler Letter at 11-12.

[47] *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.

[48] SEC, Order Approving CAT NMS Plan at 715; *see also* Data Security Proposal at 10, 85 Fed. Reg. 65990 at 65991, ("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.").

[49] *See*, *e.g.*, CAT NMS Plan § 6.2 (listing duties of Chief Compliance Officer and Chief Information Security Officer regarding monitoring and addressing data security, such as regular review of data security measures, implementing an annual audit plan, and reviewing policies and procedures of the Participants that are related to CAT cybersecurity); § 6.12 (requiring the Plan Processor to "develop and maintain a comprehensive information security program for the Central Repository, to be approved and reviewed at least annually by the Operating Committee"); Appendix C § A.4(a) (summarizing data security requirements including the requirement to designate a Chief Compliance Officer and a Chief Information Security Officer, who are in turn required to "retain independent third parties with appropriate data security expertise to review and audit on an annual basis the policies, procedures, standards, and real time tools that monitor and address data security issues for the Plan Processor and the Central Repository"); Appendix D § 4 (describing data security requirements, noting that the Plan Processor will "assess it for vulnerabilities," and providing that the security plan must be updated annually).

[50] 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.").

### D. Regulatory Immunity

#### 1) Contractual Liability Limitations and Regulatory Immunity

SIFMA acknowledges that the Participants are implementing the requirements of Rule 613 and the CAT NMS Plan in their regulatory capacities and asserts that the Participants therefore do not "need anything more than the judicial doctrine of 'regulatory immunity' to protect them in connection with their operation of the CAT."[51] The Participants disagree. As discussed in the Response Letter, the Limitation of Liability Provisions are necessary despite the applicability of regulatory immunity because of the uncertainty inherent in litigation and to avoid the costs associated with defending against potential Industry Member lawsuits before courts determine that the Participants are immune.

Although the Participants firmly believe that they are entitled to regulatory immunity while implementing the requirements of the CAT NMS Plan, there is no guarantee that all courts will agree that the Participants' immunity defense extends to the particular claims asserted.[52] This uncertainty is compounded by SIFMA's ambiguous—and elusive—position regarding the applicability of regulatory immunity to the CAT and efforts to abolish the doctrine legislatively.[53] While SIFMA acknowledges the longstanding principle that SROs are "entitled to broad immunity from private liability" when they perform regulatory functions, the SIFMA Letter does not indicate that SIFMA and its constituent Industry Members will abandon their extensive efforts to challenge the doctrine in court or cease lobbying Congress to abrogate it by statute.[54] Under these circumstances, the Participants should receive the longstanding contractual liability protections that SROs historically receive when they stand in the shoes of the Commission.

In addition to the uncertainty of the ultimate result, the *process* of litigating challenges to regulatory immunity in the event of a CAT Data breach would create substantial costs, which ultimately will be passed along to Industry Members as part of CAT LLC's joint funding, and then further to retail investors. Significantly, regulatory immunity defenses are decided on a "case-by-case basis,"[55] and the applicability of the doctrine may not be resolved until after appellate review. Litigation would be costly and resource intensive and would ultimately distract the Participants and FINRA CAT from their important regulatory oversight mandate as ordered by the

---

[51] SIFMA Letter at 6.

[52] *See* Response Letter at 22-25, Section E(3).

[53] As discussed in the Response Letter, although SIFMA now suggests that the Participants rely on regulatory immunity, SIFMA has challenged SRO immunity generally and specifically with respect to the CAT. *See id*. Moreover, it is clear that SIFMA does not speak for all of its members on this issue, as at least one prominent broker-dealer continues to assert that the Participants should not be entitled to either a contractual limitation of liability or regulatory immunity in connection with the operation of the CAT. *See* Letter from Daniel Keegan, Citi to Vanessa Countryman, Secretary, U.S. Securities and Exchange Commission, at 2-4 (Feb. 25, 2021) (the "Citi Letter"), available at https://www.sec.gov/comments/4-698/4698-8419819-229522.pdf. As such, litigation challenging regulatory immunity in the event of a CAT Data breach is all but guaranteed.

[54] *See* SIFMA Letter at 7.

[55] *DL Capital Grp.,* 409 F.3d at 97.

Commission. A contractual liability limitation—authorized pursuant to the Commission's rule-making authority—provides a necessary layer of protection against these substantial costs by ensuring that the longstanding allocation of liability between Industry Members and regulators applies to CAT reporting.

For these reasons, the SROs traditionally have sought, and received, the protection of contractual liability limitations even where their activities were likely protected by regulatory immunity. The Commission routinely has concluded—by approving limitations of liability in the rules of every SRO—that supplementing regulatory immunity with limitation of liability provisions is consistent with the Exchange Act.[56]

SIFMA also acknowledges that agreements for OATS and other NMS plans contain liability exclusions that protect the Participants, notwithstanding the high likelihood that the Participants would also be entitled to regulatory immunity in connection with those reporting facilities.[57] Nonetheless, SIFMA asserts that because the CAT receives more data than OATS and other NMS facilities receive, those contractual limitations should not inform the scope of the Limitation of Liability Provisions in the CAT Reporter Agreement.[58] The Participants are not aware of any rationale as to why the volume of data stored in the CAT should impact the appropriate allocation of liability, or why such differences would support shifting liability from Industry Members to their regulators.

2) Use of CAT Data for Commercial Purposes

SIFMA asserts that because the securities exchanges have for-profit components (in addition to their self-regulatory functions), certain unspecified "pressures" may "cause them to potentially misuse the CAT Data in a commercial manner."[59] SIFMA's speculation is baseless and certainly cannot overcome the compelling rationale for the Limitation of Liability Provisions. SIFMA also ignores that both the CAT NMS Plan and Reporter Agreement squarely prohibit the use of CAT Data for commercial purposes.[60] The Proposed Amendment does not impact these prohibitions. And to the extent that a Participant violates the CAT NMS Plan (or any other applicable Commission mandate), that entity can be subjected to an enforcement action (or other SEC action). SIFMA offers no explanation for its not-so-subtle claim that the SEC's enforcement regime is insufficient to properly incentivize the Participants to use CAT Data in accordance with the CAT NMS Plan.

---

[56] Proposed Amendment at 5-9, Section A(3); Response Letter at 5-7, Section B(1); *Id*. at 22-25, Section E(3).

[57] SIFMA Letter at 7.

[58] *Id.*

[59] *Id.*

[60] *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.").

### E. Application of the Proposed Amendment to Willful Misconduct, Gross Negligence, Bad Faith, and Criminal Acts

SIFMA asserts that the Limitation of Liability Provisions are inappropriate because they do not carve out willful misconduct, gross negligence, bad faith, or criminal acts.[61] SIFMA argues that "the lack of such carve-outs deviate from traditional contracting norms" and that the Proposed Amendment would "excuse an exchange or its representatives from liability" if they misuse CAT Data for commercial purposes or steal CAT Data for personal gain.[62] Neither of those arguments provides a basis for the Commission to exclude willful misconduct, gross negligence, bad faith, and criminal acts from the Limitation of Liability Provisions.

As an initial matter, SIFMA's argument regarding "traditional contracting norms" fails to identify the specific norms to which SIFMA refers, offer any policy rationale for those supposed norms, or explain why they would apply to a regulatory program with Commission-mandated reporting.[63] Contrary to SIFMA's position, the relevant "norms"—as reflected in SRO rules as well as other regulatory reporting facilities and NMS plans—underscore the conclusion that the Limitation of Liability Provisions in the CAT Reporter Agreement should **not** exclude willful misconduct, gross negligence, bad faith, and criminal acts.

As SIFMA belatedly appears to recognize, the liability rules of many SROs (all approved by the SEC as consistent with the Exchange Act) do not recognize these exclusions.[64] In its initial comment letter regarding the Proposed Amendment, SIFMA selectively highlighted Cboe Rule 1.10 to argue that SRO rules generally provide Industry Members with a broad right to recover damages against the Participants in the event of gross negligence, willful misconduct, or similar conduct. After reviewing the Participants' Response Letter, which contained an extensive discussion of the scope and history of SRO liability rules, SIFMA implicitly acknowledges that Cboe Rule 1.10 is not the norm for SRO liability rules.[65]

But SIFMA continues to incorrectly claim that Cboe's rules broadly provide for liability "for certain types of conduct such as gross negligence and willful misconduct."[66] Simply put, that is not an accurate characterization of Cboe's liability rules or the liability rules of any U.S. securities exchange. As discussed in the Response Letter, those SRO rules containing certain exclusions (e.g., Cboe Rule 1.10) generally are modified by other rules that broadly prohibit Industry Members from suing the exchanges or their representatives, except for violations of the federal

---

[61] SIFMA Letter at 8-9.

[62] *Id.* at 8.

[63] *Id.*

[64] *Id.*; *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.

[65] *See* SIFMA Letter at 8.

[66] *Id.* at 8.

securities laws for which a private right of action exists.[67] Accordingly, even when SRO liability rules permit certain types of claims (e.g., gross negligence and willful misconduct), Industry Members often are 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.[68] The Participants do not believe that these provisions would provide for liability against the SROs in the event of a data breach. At bottom, the Commission-approved SRO liability rules provide no support for the categorical exclusions that SIFMA advocates to be included in the Limitation of Liability Provisions.

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) generally do not contain the exclusions that SIFMA advocates to be included in the CAT Reporter Agreement.[69] The Participants are not aware of any reason to deviate from this longstanding precedent in the context of CAT reporting.

Charles River's economic analysis provides additional support for this longstanding precedent. In the CRA Reply, Charles River addressed the question of whether certain types of conduct should be excluded from the Limitation of Liability Provisions from the perspective of economic analysis.[70] Charles River concluded that the proposed exclusions are unwarranted in part because "adding commenters' proposed exclusions to the limitation of liability provisions would potentially generate substantial litigation [because] [c]ompetent litigators will likely try to satisfy pleading standards even when the facts may be inconsistent with such claims."[71] If the Commission modifies the Proposed Amendment to allow Industry Members to recover from the Participants in the event of gross negligence, recklessness, willful misconduct, or bad faith, any CAT Data breach is likely to lead to litigation in which putative plaintiffs (and their counsel) attempt to demonstrate that those exclusions apply, regardless of the facts. In the context of regulatory immunity, the courts have acknowledged this reality of civil litigation against the SROs: "It is, after all, hard to imagine the plaintiff (or plaintiff's counsel) who would—when otherwise

---

[67] *See, e.g.*, BOX Exchange LLC, Rule 7230(d); Cboe Exchange, Inc., Rule 1.15; and Miami International Securities Exchange LLC, Rule 528; *see also* Response Letter at 5-6, Section B(1) (describing additional restrictions regarding the ability of Industry Members to recover compensation pursuant to SRO liability rules).

[68] As discussed in the Response Letter, 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 disclaim liability for gross negligence and willful misconduct. *See* Response Letter at 7-8 n.29 (citing *NASDAQ OMX Grp., Inc. v. UBS Sec., 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)).

[69] *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.

[70] CRA Reply at 18-19.

[71] *Id*. at 18.

wronged by an SRO but unable to seek money damages—fail to concoct some claim of fraud…."[72] For that reason, courts analyzing regulatory immunity have held that rejecting exceptions for fraud, bad faith, gross negligence, or other categories of alleged misconduct is "a matter not simply of logic but of intense practicality since otherwise the SRO's exercise of its quasi-governmental functions would be unduly hampered by disruptive and recriminatory lawsuits."[73]

Moreover, adding carveouts to the Proposed Amendment would not alter the fundamental economic reality that CAT LLC is not equipped to compensate Industry Members in the event of a data breach.[74] CAT LLC's funding is designed to cover costs only, and its balance sheet is not intended to hold sufficient assets available to compensate Industry Members harmed by a data breach. Additionally, in approving the CAT NMS Plan, the Commission mandated that the Operating Committee "shall seek … to build financial stability to support [CAT LLC] as a going concern."[75] Considering the potential for substantial losses that may result from certain categories of low probability cyberbreaches,[76] it is difficult to imagine how CAT LLC could ensure its solvency—as required by the CAT NMS Plan—if the Commission adopts a limitation of liability with substantial exclusions like willful misconduct, gross negligence, bad faith, and criminal acts.

Finally, in arguing for various exclusions from the Limitation of Liability, SIFMA reiterates its purported guiding principle that the party in "control" of the data must bear liability for its potential misuse.[77] As discussed extensively in the Proposed Amendment and the Response Letter, securities industry norms do not support the principle that the party in possession of data should bear liability in the event of a data breach.[78] That is particularly true where, as here, the parties in possession of the data (i.e., the Participants, CAT LLC, and FINRA CAT) are acting in regulatory capacities pursuant to Commission rules. The SIFMA Letter sheds no new light on this subject.

---

[72] *See, e.g., DL Capital Grp.*, 409 F.3d at 99.

[73] *Id*. (internal quotations and citations omitted).

[74] SIFMA continues to make clear that it is primarily concerned with potential data breaches that may lead to catastrophic damages. SIFMA Letter at 8 ("For many types of market participants, access to their transaction data could lead to exposure of their sensitive and proprietary trading strategies and could allow, for example, competitors or bad actors to misuse their data or reverse engineer their trading strategies. Indeed, for certain participants, it is not a stretch to say that they view their trading history with just as much importance as individual investors view their social security numbers.").

[75] CAT NMS Plan § 11.2(f).

[76] *See* Proposed Amendment at 13; *see generally* Appendix B.

[77] *See generally* SIFMA Letter.

[78] As discussed in the Proposed Amendment and the Response Letter, many Industry Members—including commenters on the Proposed Amendment—simultaneously advocated for the principle that the party in "control" of data must bear all liability, while broadly disclaiming liability to their own retail investors in connection with sensitive customer data that Industry Members "control." *See* Proposed Amendment at 8 (citing examples of Industry Members' liability limitations); Response Letter at 10-11, Section B(3).

## F. Impact on Efficiency, Competition, and Capital Formation

### 1) Costs to Investors

SIFMA asserts that the Proposed Amendment "does not promote the Exchange Act goals of efficiency, competition and capital formation because it would ultimately lead to higher costs for investors."[79] The Participants disagree. Charles River's White Paper provides an extensive analysis indicating that the Proposed Amendment is the most efficient manner of addressing the allocation of liability in the event of a CAT Data breach, and that other approaches (such as allowing Industry Member litigation for damages) would generate few, if any, benefits while imposing substantial costs that are impossible to quantify on an *ex-ante* basis.[80]

Charles River also has identified "several marginal operating costs" that would result from eliminating a limitation of liability even in the absence of actual litigation, including costs associated with "extra-marginal defensive investments in cyber risk protection, with reduced efficacy of the CAT system due to excess, litigation-driven security measures, or a cash build-up scheme that would be borne by the Participants/SROs and Industry Members."[81] Critically, these added costs—whether resulting from litigation or any other source—ultimately would be passed along to investors (including retail investors). These added costs will "likely lead[] to reduced trading levels, reduced participation in markets by investors, or increased costs of raising capital."[82]

### 2) Insurance Considerations

SIFMA argues that CAT LLC must accept the liability for a CAT Data breach so that the Participants are "appropriately incentivized to invest in insurance and other risk mitigation measures."[83] The Participants disagree that the prospect of Industry Member litigation is needed to incentivize appropriate "insurance and other risk mitigation measures" and note that at the time CAT LLC decided to purchase the maximum available insurance that the market would viably offer at the time, 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 economically viable coverage available is not contingent on whether they are protected by a limitation of liability provision. SIFMA's argument posits a situation that does not exist (i.e., a lack of incentives for CAT to purchase insurance and implement risk mitigation measures) to argue for a solution that will not impact the CAT's insurance coverage nor meaningfully improve the CAT's cybersecurity, but will lead to higher overall costs (i.e., an absence of a contractual limitation of liability).

---

[79] SIFMA Letter at 9.

[80] *See* Appendix B at Sections III(A)-(D).

[81] Appendix B at 46.

[82] Appendix B at 47.

[83] SIFMA Letter at 10.

As it did in its January Comment Letter, SIFMA suggests—without support—that CAT LLC can simply purchase additional insurance, and requests that the Participants publicly disseminate confidential details regarding CAT LLC's insurance to enable SIFMA to evaluate the scope of coverage.[84] The Participants note that sharing this information publicly could potentially incentivize bad actors to target the CAT (e.g., with ransom demands), and would therefore be ill-advised from a risk management perspective. The Participants also reiterate that CAT LLC has purchased the maximum amount of coverage that the current market will reasonably provide. Additionally, the Participants regularly evaluate CAT LLC's insurance and intend to purchase additional coverage to the extent it becomes reasonably available.

### G. Continued Negotiations with SIFMA

On May 3, 2021, SIFMA provided the Participants with a proposal setting forth the terms upon which Industry Members would be willing to resolve the dispute regarding the allocation of liability in the event of a CAT Data breach.[85] SIFMA states that its proposal "builds on and incorporates terms" from a term sheet that the Participants previously provided to SIFMA.[86] SIFMA's May 3, 2021 response marks the first substantive response to the Participants' March 27, 2020 term sheets.[87]

The Participants appreciate SIFMA's willingness to discuss the appropriate scope of a limitation of liability provision. The Participants are reviewing the May 3 term sheet and will respond to SIFMA's proposal in due course.

---

[84] SIFMA Letter at 9, 10, 11; *see also* Letter from Ellen Greene, SIFMA to Vanessa Countryman, Secretary, U.S. Securities and Exchange Commission, at 8-9 (Jan. 27, 2021), available at https://www.sec.gov/comments/4-698/4698-8298026-228278.pdf.

[85] *Id*. at 11.

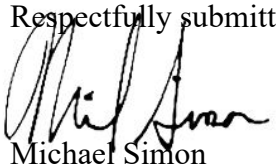
[86] *Id.*

[87] The Participants' proposals were provided to the Commission on April 1, 2020. *See* April 1, 2020 Email from M. Simon to M. Kimmel. The Participants previously summarized the negotiation history regarding limitation of liability issues. *See* Response Letter at 2-3, Section A(1).

*  *  *  *  *

Thank you for your attention to this matter. Please contact me at (212) 229-2455 if you have any questions or comments.

Respectfully submitted,



Michael Simon
CAT NMS Plan Operating Committee Chair

cc: The Hon. Gary Gensler, Chair
The Hon. Allison Herren Lee, Commissioner
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
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