CITADEL | Securities

February 23, 2021

Ms. Vanessa A. Countryman
Secretary
Securities and Exchange Commission
100 F Street NE
Washington, DC 20549–1090

**Re: Proposed Amendments to the National Market System Plan Governing the Consolidated Audit Trail (File No. 4-698)**

Dear Ms. Countryman:

Citadel Securities appreciates the opportunity to provide comments to the Securities and Exchange Commission ("Commission" or "SEC") on the proposal submitted by the participants ("Participants") to the national market system plan governing the consolidated audit trail ("CAT NMS Plan") to insert limitation of liability provisions ("Provisions") into the CAT NMS Plan ("Proposal").[1]

Previously, the Participants sought to eliminate any potential liability for themselves, the consolidated audit trail plan processor, CAT NMS, LLC ("CAT LLC"), and their representatives[2] for any damages associated with the consolidated audit trail ("CAT") by inserting the Provisions into the CAT Reporter Agreement, an agreement that each broker-dealer required to report to the CAT ("CAT Reporter") was obligated to sign before being granted the ability to report data to the CAT. After multiple CAT Reporters objected to signing the agreement with these terms, noting, among other things, that the Participants had not adopted a requirement to sign the agreement, the Participants settled the matter by withdrawing the Provisions and allowed the CAT Reporters to sign an agreement without the objectionable Provisions. The Proposal now seeks to re-introduce the same Provisions by filing them as part of an amendment to the CAT NMS Plan. As support for the Proposal, the Participants have appended a white paper ("White Paper") authored by Charles River Associates ("Charles River") purporting to demonstrate the necessity for the Provisions.

The Proposal should be rejected for two primary reasons. First, the Provisions are unnecessary—and against good public policy—given that the Participants are already shielded from liability when performing their regulatory obligations under the doctrine of regulatory immunity—a fact all but completely ignored in both the Proposal and the White Paper. Second, the White Paper's analysis is flawed and rests on a number of erroneous premises. In fact, as

---

[1] Securities Exchange Act Release No. 90826 (Dec. 30, 2020), 86 FR 591 (Jan. 6, 2021).

[2] The term "representatives" includes "EACH OF THE PARTICIPANTS, THE PLAN PROCESSOR AND ANY OTHER SUBCONTRACTORS OF THE PLAN PROCESSOR OR CATLLC PROVIDING SOFTWARE OR SERVICES IN CONNECTION WITH THE CAT SYSTEM, AND ANY OF THEIR RESPECTIVE AFFILIATES AND ALL OF THEIR DIRECTORS, MANAGERS, OFFICERS, EMPLOYEES, CONTRACTORS, SUBCONTRACTORS, ADVISORS AND AGENTS." *See* Proposal at 28 (proposed Section 5.5 of the Provisions).

described below, we believe that the framework adopted by the White Paper (i.e., weighing the costs and benefits of imposing *ex-ante* regulation and/or *ex post* litigation) demonstrates that permitting litigation against the Participants and their representatives when they are acting outside their regulatory capacity is crucial, as having potential liability for data security failures would give the Participants very strong financial incentives to invest heavily in steps to prevent or minimize the likelihood or impact of such failures.

## 1. Background

The Commission, the Participants, and all industry members agree that the data security of the CAT is of critical importance. One essential aspect of this security is protecting against a cybersecurity breach of the CAT itself, but it is only *one* aspect of the data security issues presented by the CAT. The Commission and the Participants have taken numerous steps to secure the CAT, and the CAT NMS Plan itself includes several provisions focused on the security of the CAT databases. Although Citadel applauds those efforts and has voiced its support for those provisions, the Participants have also supported provisions in the CAT NMS Plan that would imperil the security of data submitted to the CAT. One fundamental data security concern that has been raised on multiple occasions by numerous parties, including Citadel, surrounds the Participants' ability to extract data and store it outside of the CAT.[3] Once a Participant moves CAT data outside the CAT, the CAT's cybersecurity policies and all of the associated bells and whistles the CAT has put into place become obsolete: the data is controlled and protected by the Participant that has extracted it, not CAT LLC. Recognizing the profound risks this creates, the Commission in August 2020 proposed enhancements to the security of CAT data, which included proposed amendments to the CAT NMS Plan designed to improve the security of CAT data that is extracted from the CAT by a Participant.[4] Citadel strongly supported the Commission's proposals and offered several suggestions that we believe would further enhance the security of CAT data. Meanwhile, Nasdaq, Cboe, ICE—which together represent a majority of the Participants—and the CAT NMS Plan Operating Committee ("CAT OC") itself all filed comment letters opposing the proposed amendments (while stressing the importance of CAT data security).

The Participants' goals in proposing the Provisions while objecting to the Commission's recent proposed amendments as they relate to CAT data security are clear: they want the unfettered ability to extract and store data from the CAT outside the CAT itself while, at the same time, having complete immunity from *any* liability should anything happen to that data as a result of their actions, be it gross negligence in securing the data or misuse by an internal bad actor. This is a fundamental disconnect that runs throughout the Proposal: the Proposal focuses on CAT LLC, the existing security provisions in the CAT NMS Plan that apply to the CAT itself and the data inside the CAT while, at the same time, proposing Provisions that extend far beyond that and cover not only CAT LLC but also the Participants and their representatives (among others) and CAT

---

[3] *See, e.g.*, Letter to Vanessa A. Countryman, Secretary, SEC from Stephen John Berger, Managing Director, Global Head of Government & Regulatory Policy, Citadel Securities (Nov. 30, 2020); Letter to Brett Redfearn, Director, Trading and Markets, SEC from Stephen John Berger, Managing Director, Global Head of Government & Regulatory Policy, Citadel Securities (June 1, 2020).

[4] *See* Securities Exchange Act Release No. 89632 (Aug. 21, 2020), 85 FR 65990 (Oct. 16, 2020) ("CAT Security Proposal").

data that is extracted, stored, and used outside the purported enhanced safety of the CAT environment.[5]

For example, the Proposal goes to great lengths to establish that the Provisions are necessary to protect CAT LLC from insolvency noting that:

> [t]o that end, CAT LLC has obtained the maximum extent of cyber-breach insurance coverage available and has implemented a full cybersecurity program to safeguard data stored in the CAT, as required by Rule 613 and the Plan. Nevertheless, considering the potential for substantial losses that may result from certain categories of low probability cyberbreaches, 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.[6]

The Provisions, however, do not apply only to CAT LLC; they apply to potential liability regarding "CAT LLC, *the Participants, and their respective representatives* to any individual CAT Reporter or CAT Reporting Agent to the lesser of the fees actually paid to CAT for the calendar year or $500."[7] These are not provisions only to protect the solvency of CAT LLC; they are provisions to protect the Participants and their representatives, including from any and all potential misuse, including intentional misuse, of CAT data. This would be a profound extension of liability limitation.

For the reasons set forth below, the Commission should reject this effort by the Participants to shield themselves and their representatives from virtually any liability.

**2. The Proposal is unnecessary in light of the Participants' status as self-regulatory organizations that have immunity for conduct undertaken when performing regulatory obligations.**

The Commission should reject the Proposal because the Provisions would insulate the Participants and their representatives when engaging in misconduct outside their regulatory responsibilities. The Participants assert that the need for the Provisions is "particularly compelling where, as here, the Participants and CAT LLC are implementing the requirements of the CAT NMS Plan in their regulatory capacities."[8] In fact, it is precisely the opposite: when the

---

[5] This distinction manifests itself in the White Paper as well. *See, e.g.*, Proposal at 34 ("In deciding whether to approve Participants' proposed plan amendment, an important question for the SEC to address is whether, *in light of the extensive cyber requirements already imposed on CAT LLC* through regulation, the SEC-mandated nature of the CAT, and the ability of the SEC to bring enforcement actions to compel compliance, it is appropriate to also allow Industry Members to sue CAT LLC *and the Participants*.") (emphasis added).

[6] Proposal at 15.

[7] *Id.* at 8.

[8] *Id.* at 12.

Participants are acting in their regulatory capacities, as self-regulatory organizations ("SROs"), they are *already* immune from liability for their conduct, and the Provisions are superfluous.[9] . But a Participant and its representatives should not be shielded from liability for all conduct—and even misconduct—concerning the CAT simply because the Participant is also a regulator. What we object to is granting the Participants and their representatives absolute immunity for activity outside of the scope of their regulatory activities through contract terms that CAT Reporters have no choice but to sign. Indeed, the Commission recently reiterated that the CAT should be used only for regulatory purposes; any use of the CAT or of CAT data for purposes outside of that scope is not permitted.[10]

As established by case law, as SROs, the Participants are immune from liability for conduct falling within the scope of their regulatory and general oversight functions delegated to them by the Commission under the Securities Exchange Act of 1934 ("Exchange Act").[11] The Exchange Act contemplates that SROs will perform a variety of regulatory functions, including examining for compliance with securities laws and promulgating and enforcing rules governing the conduct of their members.[12] It is settled law that, because SROs "perform a variety of vital governmental functions, but lack the sovereign immunity that governmental agencies enjoy, SROs are protected by absolute immunity when they perform their statutorily delegated adjudicatory, regulatory, and prosecutorial functions."[13] However, recognizing that it would be against good public policy to grant SROs absolute immunity involving all of their conduct merely due to their status as SROs, it is only when an SRO is "acting under the aegis of the Exchange Act's delegated authority," that

---

9 Aside from a passing, oblique reference in a footnote to the doctrine of regulatory immunity, neither the Proposal nor the White Paper addresses the existence of this doctrine. *See id.* at 7 n.14 ("The modifications in this Proposed Amendment are not intended to and do not affect the limitations of liability set forth in the agreements between individual Participants and Industry Members or SEC-approved rules regarding limitations of liability, or those limitations *or immunities that bar claims for damages against the Participants and CAT LLC as a matter of law*.") (emphasis added).

10 In this regard, we reaffirm our support for the Commission's recent efforts to clarify the appropriate use of CAT data by the Participants and that such use be limited to purely surveillance and regulatory purposes with no commercial purpose. *See* CAT Security Proposal, at 217 ("The Commission believes that it is important that CAT Data be used only for surveillance and regulatory purposes. The Commission also believes it is important to prohibit Participants from using CAT Data in situations where use of CAT Data may serve both a surveillance or regulatory purpose, and commercial purpose, and, more specifically prohibit use of CAT Data for economic analyses or market structure analyses in support of rule filings submitted to the Commission pursuant to Section 19(b) of the Exchange Act ('SRO rule filings') in these instances.").

11 *Weissman v. Nat'l Ass'n of Secs. Dealers, Inc.*, 500 F.3d 1293 (11th Cir. 2007).

12 *See, e.g.*, Exchange Act, §§ 6(b), 15A(b)(2).

13 *Weissman*, 500 F.3d at 1296 (citing *Barbara v. N.Y. Stock Exch.*, 99 F.3d 49, 59 (2nd Cir. 1996); *Austin Mun. Sec., Inc. v. Nat'l Ass'n of Secs. Dealers, Inc.*, 757 F.2d 676, 692 (5th Cir. 1985); *Sparta Surgical Corp. v. Nat'l Ass'n of Secs. Dealers, Inc.*, 159 F.3d 1209, 1215 (9th Cir. 1998); *Zandford v. Nat'l Ass'n of Secs. Dealers, Inc.*, 80 F.3d 559, 559 (D.C. Cir. 1996)).

it enjoys that privilege, and "entities that enjoy absolute immunity when performing governmental functions cannot claim that immunity when they perform non-governmental functions."[14]

Consequently, to the extent an SRO engages in non-governmental activities, including those that serve its private business interests, the SRO does not have immunity from lawsuits.[15] Quite simply, the law favors providing legal remedies to injured parties, and therefore grants of immunity are narrowly construed, meaning that courts must be "careful not to extend the scope of the protection further than its purposes require."[16] As the Eleventh Circuit explained:

> [E]ntities that enjoy absolute immunity when performing governmental functions cannot claim that immunity when they perform non-governmental functions. For example, municipal corporations may enjoy the same level of immunity as the government itself when "acting in their governmental capacity. . . . When, however, they are not acting in the exercise of their purely governmental functions, but are performing duties that pertain to the exercise of those private franchises, powers, and privileges which belong to them for their own corporate benefit, . . . then a different rule of liability is applied and they are generally held responsible for injuries arising from their negligent acts or their omissions to the same extent as a private corporation under like circumstances." The dual nature of SROs as private companies that carry out governmental functions is similar to that of municipal corporations.[17]

The same should be true of extra-governmental functions, such as misuse of data. Although the Proposal takes great pains to present the Participants as potentially subject to substantial liability simply for fulfilling their regulatory mission, this is simply not the case. The issue the Commission must consider is not whether the Participants should be liable for conduct undertaken during the course of their regulatory responsibilities; they are not. Rather, the issue the Commission must decide is whether to approve the Provisions that are intended to insulate the Participants and their representatives from any potential liability arising "under [the] agreement" CAT Reporters must sign that would not be covered by regulatory immunity. Citadel submits that such sweeping immunity from liability is not in the public interest or consistent with the Exchange Act.

---

[14] *Weissman*, 500 F.3d at 1297; *see also Huntley v. Chicago Bd. Options Exch.*, Fed. Sec. L. Rep. ¶ 98,880 (N.D. Ill. 2015) ("The purpose of absolute immunity is to protect all conduct of an SRO from liability, so long as the conduct arises out of the discharge of its duties under the Exchange Act.").

[15] *See City of Providence v. BATS Global Markets, Inc.*, Fed. Sec. L. Rep. ¶ 98,880 (2nd Cir. 2017); *Weissman*, 500 F.3d at 1299; *In re Facebook, Inc. IPO Sec. & Derivative Litig.*, 986 F.Supp.2d 428, 452 (S.D.N.Y. 2013).

[16] *Weissman*, 500 F.3d at 1297 (citing *Forrester v. White*, 484 U.S. 219, 224 (1988); *see also Owen v. City of Independence*, 445 U.S. 622, 645 n.28 (1980)) (internal citations omitted).

[17] *Weissman*, 500 F.3d at 1296 (citing *Owen*, 445 U.S. at 645 n.27 (quoting W. Williams, Liability of Municipal Corporations for Tort § 4, at 9 (1901))).

**2. The White Paper does not support the Participants' conclusion that the Provisions are necessary.**

As described in the Proposal, "CAT LLC retained Charles River to conduct an economic analysis of liability issues in relation to a theoretical CAT data breach."[18] The Participants described the White Paper as consisting of two principal components:

> First, Charles River identified specific potential breach scenarios that could impact the CAT, and quantified the likelihood and potential financial magnitude of each scenario. Second, Charles River applied economic principles regarding the costs and benefits of litigation to the question of whether a limitation of liability should appropriately be included in the Reporter Agreement.[19]

In conducting this analysis, Charles River sought to address "whether the cyber risk posed by CAT should be addressed through *ex-ante* regulation, *ex post* litigation, or a combination of both approaches."[20] The Participants conclude that the White Paper "supports CAT LLC's and the Participants' decision to limit their liability to Industry Members."[21] In fact, it does not.

The first flaw with the White Paper is that it is focused on too narrow a set of security concerns. The White Paper focuses largely on cybercrime and, while it acknowledges the risks presented by internal bad actors, the analysis is focused almost exclusively on an assessment of an external malicious actor's ability to "hack" into one or more of the CAT databases.[22] The White Paper fails to sufficiently address other likely scenarios, such as the misuse of CAT data by an individual at a Participant, or any representatives of the Participant who *already* have access to the CAT. In such circumstances, there is no need to "hack" into the database; access already exists. Moreover, the Participants have included a requirement in the CAT NMS Plan that the CAT support a minimum of 3,000 regulatory users, so the risks of potential misuse when thousands of individuals have access are hardly insubstantial.

The second, and more significant, flaw with the White Paper is that it focuses solely on a hacker's ability to obtain access to one or more of the databases maintained by CAT LLC. As noted above, one primary concern that industry members have repeated throughout the process of developing and implementing the CAT is the ability of the Participants to extract data from the CAT on a bulk download basis. This creates significant additional opportunities for hackers to access CAT data from databases *not* maintained by CAT LLC. The Commission has proposed

---

18 Proposal at 16.

19 *Id.* at 16.

20 *Id.* at 33.

21 *Id.* at 16.

22 The White Paper, for example, cites a 2020 report by Verizon indicating that almost one third of breaches were initiated by internal actors. *See id.* at 40 (citing a 2020 report by Verizon showing that "approximately 70% of breaches in 2019 were caused by external actors with the other 30% being initiated by internal actors").

amendments to the CAT NMS Plan to help alleviate some of the concerns with bulk downloading; however, the proposal—which, as noted, generated multiple negative comment letters from the Participants and from the CAT OC—is still pending with the Commission. Although the ability to hack into a CAT database is of key importance, a larger concern is the ability of a malicious actor to obtain access to databases *not* maintained by CAT LLC, i.e., maintained by a Participant that has extracted such data in bulk form or otherwise.

Using this woefully incomplete threat analysis, Charles River applied it to a framework to determine whether it would be best for the Commission "to address the question of whether it is economically optimal to mitigate CAT LLC's cyber risk exposure (and the potential resulting harm to third parties) through regulation or through litigation, or through some combination of the two methods."[23] Charles River concluded that "regulation alone is preferable to regulation plus litigation."[24] We believe this conclusion is inherently flawed and that, in fact, permitting litigation when the Participants are acting outside of the conduct to which regulatory immunity would attach is significantly more appropriate than having the Participants have no threat of liability because all CAT Reporters have been forced to sign away their ability to litigate. Facing potential liability for data security failures would give the Participants very strong financial incentives to invest heavily in steps to prevent or minimize the likelihood or impact of such failures

As Charles River observes, "[e]conomists (and others) have long recognized that the prospect of being held legally liable for harm *ex post* provides incentives for the relevant parties to take care *ex-ante,* thereby reducing the likelihood or the expected severity of an adverse event injuring either the first party or third parties."[25] While seeking to distinguish instances where both *ex-ante* regulation and *ex post* litigation are used, the White Paper states that:

> In the situation faced by the CAT, the SEC has already concluded that the existing cyber security framework is adequate and they can amend the regulatory scheme to require additional cyber security measures to enhance the ex-ante protection against cyber breaches, to the extent permitted by applicable laws and regulations. Indeed, the SEC has pursued this path on multiple occasions.[26]

The White Paper also suggests that SEC oversight, coupled with enforcement risk, is sufficient to outweigh any incremental benefit that comes from also allowing private *ex post* litigation.[27]

---

23 *Id.* at 65.

24 *Id.* at 66.

25 *Id.*

26 *Id.* at 70.

27 *Id.* at 73. Specifically, the White Paper states that "[t]he SEC can also require CAT LLC and the Participants to amend their cyber policies, procedures, systems and controls in response to subsequent developments or newly identified vulnerabilities, to the extent consistent with applicable laws and regulations. In addition, it is important to recognize that the SEC may bring enforcement actions against Participants and the CAT should they fail to comply with best practices embodied in the CAT NMS Plan or SEC regulations, including Regulation SCI."

This reasoning is flawed in a number of respects. First, 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. Moreover, and in direct contrast to the statements in the White Paper, the Commission's recently proposed enhancements to CAT security demonstrate that the Commission in fact has NOT "concluded that the existing cyber security framework is adequate."[28] Rather, the Commission has determined it may be necessary to enhance the security of the CAT and has proposed amendments to the CAT NMS Plan to do exactly that. Ironically, the proposal cited by Charles River includes the very same amendments to which many of the Participants and the CAT OC object. Using the framework provided by Charles River, this would seem to underscore the importance of allowing *ex post* litigation, as opposed to limiting all liability.[29]

Indeed, the very proposed amendment cited in the White Paper demonstrates a second flaw: altering behavior through regulation is a slow, uncertain process. In addition to the time needed to develop, approve, and publish the proposal cited by Charles River (i.e., the CAT Security Proposal), it has been pending for five months after being published. Even if the proposal is approved, there will likely be a protracted implementation period before the amendments are effective. Given the constantly evolving changes to technology and cybersecurity threats, the idea that regulation can keep pace with data security issues and motivate behavior is naïve at best.

The White Paper itself highlights another flaw in the Proposal as it relates to insurance. The White Paper discusses the importance of insurance to address potential breach scenarios, which is a crucial component of an assessment of potential liability.[30] Although the Proposal states that CAT LLC has obtained insurance, it provides no details regarding the insurance, such as the amount or type of coverage, what is covered, or to whom it applies. Moreover, there is no analysis as to whether the Participants, rather than CAT LLC, should likewise seek insurance from potential litigation due to a data breach or the effect such insurance could have on the Participants'

---

[28] *See* CAT Security Proposal, at 10 (noting that "the Commission believes that it can and should take additional steps to further protect the security and confidentiality of CAT Data" and therefore proposing "to amend the CAT NMS Plan to enhance the security of the CAT and the protections afforded to CAT Data").

[29] For example Charles River states:

> One way that the reliance upon rules becomes problematic is when it is difficult to write a precise *ex-ante* rule that considers all possible circumstances that might be associated with the context of the loss. In such cases, it is likely the resulting standard will either be vague, highly complex, or will not consider every possible situation that might arise when the loss producing event occurs. *Ex post* litigation may be preferred in these situations so that judgement regarding the circumstances of the loss can be more easily considered as part of the adjudication process.

Proposal at 67. The current circumstances, in which the Participants and the SEC are debating whether the SEC's proposed security enhancements would improve or (as the Participants believe) diminish the security of the CAT evidences the difficulties of creating robust *ex-ante* rules.

[30] *See* Proposal at 84-87.

incentives to protect data that they extract from the CAT and store outside the CAT. Without these essential details, it does not permit the Commission or the public to adequately evaluate the Proposal against the analysis Charles River performed.

Portions of the White Paper also misstate aspects of industry input into issues involving CAT security. For example, Charles River significantly overemphasizes the visibility and input into the workings of the CAT provided to the industry. The White Paper states that "[t]here is a level of participation and information flow from and to the Industry Members (and other potentially interested groups) through the Advisory Committee, and previously the Development Advisory Group, and an attendant ability to influence the business operation and cyber security investments and practices that is not typically found in conventional business relationships."[31]

This too is incorrect. Although 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. As we and others noted in our comment letters on the CAT Security Proposal, we believe industry members should be added to the CAT Security Working Group (again, a position with which the Participants do not agree).[32] This would seem to provide yet further evidence of why *ex post* litigation is a needed remedy under the circumstances.

Finally, it is spurious to assert that *ex post* litigation would provide only incremental benefit to the authority of the SEC to regulate and bring enforcement actions against the Participants. The White Paper cites as examples potential actions brought by the SEC against the Participants for violations of the CAT NMS Plan or Regulation SCI. These examples involve SEC enforcement of what are primarily procedure-based requirements; that is, these provisions require Participants to establish reasonably designed written policies and procedures. Thus, if a failure to protect CAT data occurs even with such policies and procedures in place, the Participants have no liability under those provisions. From a liability perspective, the Participants have the incentive to comply with the applicable requirements, but no more: provided they meet the regulatory minimum standard, no liability can attach. We believe that the prospect of private litigation substantially increases the

---

[31] *Id.* at 39; *see also id.* at 77 ("In addition, the Industry Members are designated members of the Advisory Committee, which gives them access to substantial information about the cyber security circumstances at the CAT and the Plan Processor.").

[32] *See* Letter from Stephen John Berger, Managing Director, Global Head of Government and Regulatory Policy, Citadel Securities, to Vanessa A. Countryman, Secretary, SEC, at 7 (Nov. 30, 2020) ("We recommend that the [Security Working Group] be enhanced by expanding its composition to include CISOs from the broker-dealer community or other similar outside experts."); *see also* Letter from Ellen Greene, Managing Director, Securities Industry and Financial Markets Ass'n, to Vanessa Countryman, Secretary, SEC, at 9 (Nov. 30, 2020) ("SIFMA believes that the Security Working Group could greatly benefit from the permanent inclusion of industry representatives with voting rights in the group."). By contrast, the Participants oppose industry participation on the Security Working Group. *See*, Letter from Michael Simon, CAT NMS Operating Committee Chair, to Vanessa Countryman, Secretary, SEC, at 10 (Dec. 4, 2020) ("The Participants have met with industry representatives on an ad hoc basis to discuss security matters, which has allowed the Participants to obtain the industry's views on security issues when necessary and appropriate. . . . The Participants believe that this flexibility and the current structure and operation of the Security Working Group functions extremely well without introducing unnecessary security risk to the CAT by expanding the Security Working Group beyond representatives of regulated entities.").

incentives to the Participants to ensure protections beyond just those that may simply be "reasonably designed" or required by regulation.

* * * * * * *

Citadel Securities appreciates the opportunity to provide comments on the Proposal. Please feel free to contact us with any questions regarding these comments.

Respectfully,

/s/ Stephen John Berger

Managing Director

Global Head of Government & Regulatory Policy