SECURITIES AND EXCHANGE COMMISSION
(Release No. 34-90826; File No. 4-698)

December 30, 2020

Joint Industry Plan; Notice of Filing of Amendment to the National Market System Plan Governing the Consolidated Audit Trail by 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., Miami International Securities Exchange LLC, MEMX, 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.

I. Introduction

On December 18, 2020, the Operating Committee for Consolidated Audit Trail, LLC ("CAT LLC"), on behalf of the following parties to the National Market System Plan Governing the Consolidated Audit Trail (the "CAT NMS Plan" or "Plan"):[1] 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., Miami International Securities Exchange LLC, MEMX, 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. (collectively, the "Participants," "self-regulatory organizations," or "SROs") filed with the Securities and Exchange Commission ("SEC" or "Commission") pursuant to Section 11A(a)(3) of the

[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 Securities Exchange Act Release No. 79318 (November 15, 2016), 81 FR 84696 (November 23, 2016).

Securities Exchange Act of 1934 ("Exchange Act"),[2] and Rule 608 thereunder,[3] a proposed amendment to the CAT NMS Plan that would authorize CAT LLC to revise the Consolidated Audit Trail Reporter Agreement (the "Reporter Agreement") and the Consolidated Audit Trail Reporting Agent Agreement (the "Reporting Agent Agreement") to insert the limitation of liability provisions (the "Limitation of Liability Provisions"), as contained in Appendix A, attached hereto.[4] The Commission is publishing this notice to solicit comments from interested persons on the amendment.[5]

II. Description of the Plan

Set forth in this Section II is the statement of the purpose and summary of the amendment, along with information required by Rule 608(a)(4) and (5) under the Exchange Act,[6] substantially as prepared and submitted by the Participants to the Commission.[7]

A. Statement of Purpose of the Amendment to the CAT NMS Plan

The Proposed Amendment adds industry-standard Limitation of Liability Provisions to the Reporter Agreement and Reporting Agent Agreement.[8] The Limitation of Liability

---

2 15 U.S.C 78k-1(a)(3).

3 17 CFR 242.608.

4 See Letter from Michael Simon, Chair, CAT NMS Plan Operating Committee, to Ms. Vanessa Countryman, Secretary, Commission, dated December 18, 2020. The Participants state that these provisions would address the liability of CAT LLC and the Participants in the event of a CAT data breach. The Participants further state that in conjunction with this proposed amendment (the "Proposed Amendment") to the CAT NMS Plan, each Participant intends to file with the Commission corresponding proposed changes to its individual CAT Compliance Rules.

5 17 CFR 242.608.

6 See 17 CFR 242.608(a)(4) and (a)(5).

7 See supra note 4. Unless otherwise defined herein, capitalized terms used herein are defined as set forth in the CAT NMS Plan.

8 The Participants believe that the CAT NMS Plan and certain individual self-regulatory organization rules already authorize the inclusion of the Limitation of Liability

Provisions are appropriately tailored, consistent with longstanding principles regarding allocation of liability between self-regulatory organizations ("SROs") and Industry Members, and have been agreed to in substance by virtually all Industry Members in connection with Order Audit Trail System ("OATS") reporting.

Moreover, CAT LLC has retained Charles River Associates ("Charles River") to conduct a comprehensive economic analysis of the liability issues presented by a potential CAT data breach. That analysis, attached to this Proposed Amendment as Appendix B, concludes that combining ongoing Commission oversight with a limitation on liability is the most efficient manner of addressing the complex issues presented by such potential breaches. Although Industry Members have advocated for an approach that would allow them (and their clients) to sue CAT LLC and the Participants in the event of a breach, the Charles River analysis demonstrates that this approach would significantly increase CAT LLC's costs—potentially without bounds—without any corresponding benefit to the Commission, investors, or other stakeholders, and likewise would not materially improve the security of the data transmitted to and stored within the CAT. Charles River also concludes that in light of the CAT's extensive cybersecurity (among other reasons), most potential breach scenarios, including the possibility of reverse engineering of Industry Members' trading algorithms, are relatively low-frequency events. For those reasons, and as discussed in detail below, there is no economic basis to deviate from industry norms by shifting liability from Industry Members to the Participants.

1. Background

Provisions in the Reporter Agreement and the Reporting Agent Agreement. See generally, May 6, 2020 CAT LLC Memo of Law in Opposition to SIFMA'S Motion to Stay, Admin. Proc. File No. 3-19766. The Participants nonetheless submit this Proposed Amendment to provide industry members ("Industry Members") and other interested constituencies with an opportunity to comment on the Limitation of Liability Provisions.

On July 11, 2012, the Commission adopted Rule 613 of Regulation NMS to enhance regulatory oversight of the U.S. securities markets. The rule directed the Participants to create a "Consolidated Audit Trail" (also referred to herein as the "CAT") that would strengthen the ability of regulators—including the Commission and the SROs—to surveil the securities markets.[9] Following the adoption of Rule 613, the Participants prepared and proposed the CAT NMS Plan and then implemented the Plan's extensive requirements, including its cybersecurity requirements. The Commission approved that Plan in November 2016, concluding that it incorporates "robust security requirements" that "provide appropriate, adequate protection for the CAT Data."[10]

In preparation for the launch of initial CAT equities reporting, in August 2019 the Participants shared with CAT LLC's Advisory Committee a draft Reporter Agreement.[11] Among other provisions, the draft Reporter Agreement contained an industry-standard limitation of liability provision that provided:

> TO THE EXTENT PERMITTED BY LAW, UNDER NO CIRCUMSTANCES SHALL THE TOTAL LIABILITY OF CATLLC OR ANY OF ITS REPRESENTATIVES TO CAT REPORTER UNDER THIS AGREEMENT FOR ANY CALENDAR YEAR EXCEED THE LESSER OF THE TOTAL OF THE FEES ACTUALLY PAID BY CAT

---

9 See 17 CFR 242.613 (2012).

10 SEC, Joint Industry Plan; Order Approving the National Market System Plan Governing the Consolidated Audit Trail, Release No. 34-79318; File No. 4-698, at 715 (Nov. 15, 2016), https://www.sec.gov/rules/sro/nms/2016/34-79318.pdf.

11 The Advisory Committee is comprised of broker-dealers of varying sizes and types of business, a clearing firm, an individual who maintains a securities account, an academic, institutional investors, an individual with significant and reputable regulatory expertise, and a service bureau that provides reporting services to one or more CAT Reporters. *See* CAT NMS Plan, Section 4.13(b). The Advisory Committee provides a forum for Industry Members (among other constituencies) to stay informed about, and to provide feedback to the Participants and the Operating Committee regarding, the operation and administration of the CAT. See CAT NMS Plan, Section 4.13(d)-(e).

REPORTER TO CATLLC FOR THE CALENDAR YEAR IN WHICH THE CLAIM AROSE OR FIVE HUNDRED DOLLARS ($500.00). *See id.* § 5.5.

On August 29, 2019, CAT LLC's Operating Committee approved the then-draft Reporter Agreement—including the limitation of liability—by unanimous written consent.[12]

Following the approval process, the Securities Industry and Financial Markets Association ("SIFMA") objected on behalf of certain Industry Members to the Reporter Agreement's limitation of liability provisions, particularly in relation to a potential CAT data breach. The Participants attempted to engage in a constructive dialogue with SIFMA and offered several proposed revisions to the limitation of liability provisions to address SIFMA's concerns. Among other proposals, the Participants offered: 1) to create a reserve (funded jointly by Industry Members and the Participants) to cover damages in the event of a data breach and 2) to revise the limitation of liability provision to conform with analogous provisions in the agreements that Industry Members require their retail customers to execute. Throughout those discussions, the Participants repeatedly stated that they were willing to consider any proposals offered by Industry Members whereby a limitation of liability provision would remain in the Reporter Agreement. SIFMA did not offer any substantive counterproposals; instead, it maintained its wholesale objection to any limitation of liability.

Notwithstanding SIFMA's objections, between September 2019 and May 5, 2020, over 1,300 Industry Members executed the then-operative Reporter Agreement containing the limitation of liability provision. In advance of the initial equities reporting deadline, all CAT Reporters were required to test their ability to upload data to the CAT database and then

---

[12] "[T]he Operating Committee shall make all policy decisions on behalf of the Company in furtherance of the functions and objectives of the Company under the Exchange Act, any rules thereunder, including SEC Rule 613, and under this Agreement." CAT NMS Plan, Section 4.1.

complete a certification form. To enable the approximately 60 Industry Members who did not execute the Reporter Agreement to complete the testing and certification process, CAT LLC permitted them to test with obfuscated data pursuant to a "Limited Testing Acknowledgment Form."

In March and April 2020, 10 of those 60 Industry Members rescinded their execution of the Limited Testing Acknowledgement Forms and attempted to report production data to the CAT. Because those Industry Members had not executed the Reporter Agreement, FINRA CAT (i.e., the Plan Processor) refused to permit them to submit production data. On April 22, 2020, SIFMA filed an 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"). SIFMA's application alleged that the Participants improperly required Industry Members to execute a Reporter Agreement as a prerequisite to submitting data to the CAT and that the agreement's limitation of liability provision was "unfair, inappropriate, and bad policy."[13] Contemporaneously with the filing of the Administrative Proceeding, SIFMA moved for a stay of the requirement that Industry Members sign a Reporter Agreement, or in the alternative, asked the Commission to further delay the launch of CAT reporting on June 22, 2020. On May 13, SIFMA and the Participants informed the Commission that the parties reached a settlement of the

[13] SIFMA also challenged the Reporter Agreement's provision that required Industry Members to indemnify CAT LLC and the Participants from third party claims arising from an Industry Member's unlawful acts and omissions including a failure: 1) by an Industry Member to protect and secure PII under its control, 2) of an Industry Member to protect its own systems from misuse, or 3) of an Industry Member to comply with its obligations under the Reporter Agreement. All CAT Reporters and CAT Reporting Agents (as defined in each of the Reporter Agreement and the Reporting Agent Agreement) eventually signed an Agreement that contained these industry standard indemnification provisions.

Administrative Proceeding and requested that the Commission dismiss SIFMA's application. On May 14, the Commission granted the parties' dismissal request.

The settlement between SIFMA and the Participants did not resolve the underlying disagreement regarding the proper allocation of liability in the event of a loss due to a breach of the CAT. Rather, the settlement provided a path for the minority of Industry Members that had not signed the original Reporter Agreement to test data and, subsequently, report live production data to the CAT. In particular, the settlement permitted Industry Members to report data to the CAT pursuant to a revised Reporter Agreement that does not contain a limitation of liability provision, while the Participants prepared a filing with the Commission to resolve the parties' underlying disagreement regarding the proper allocation of liability. CAT LLC's and the Participants' decision to resolve the Administrative Proceeding was animated by a desire to progress unimpeded toward the CAT's June 22 compliance date.

Initial equities reporting commenced as planned on June 22, 2020. Since that time, Industry Members have been transmitting data to the CAT pursuant to the revised Reporter Agreement, which does not contain any limitation of liability provision.

2. The Limitation of Liability Provisions

The Limitation of Liability Provisions in this Proposed Amendment, each of which was included (in substance) in the original Reporter Agreement and Reporting Agent Agreement, are contained in Appendix A to this Proposed Amendment.[14] In sum and substance, the Limitation of Liability Provisions:

---

[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.

- Provide that CAT Reporters and CAT Reporting Agents accept sole responsibility for their access to and use of the CAT System, and that CAT LLC makes no representations or warranties regarding the CAT system or any other matter;
- Limit the liability of 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;
- Exclude all direct and indirect damages; and
- Provide that CAT LLC, the Participants, and their respective representatives shall not be liable for the loss or corruption of any data submitted by a CAT Reporter or CAT Reporting Agent to the CAT System.[15]

2. The Limitation of Liability Provisions Reflect Longstanding Principles of Allocation of Liability Between Industry Members and Self-Regulatory Organizations

Limitations of liability are ubiquitous within the securities industry and have long governed the economic relationships between self-regulatory organizations and the entities that they regulate. The Limitation of Liability Provisions at issue here fall squarely within industry norms.

For over half of a century, U.S. securities exchanges have adopted rules to limit their liability for losses that Industry Members incur through their use of exchange facilities.[16] These

---

15 Appendix A also contains language clarifying the entities to which the Limitation of Liability Provisions apply. *See* Appendix A at § 5.5.

16 See, e.g., Securities Exchange Act Release No. 14777 (May 17, 1978) (SR–CBOE–78–14) (noting that an exchange ''cannot proceed with innovative systems and procedures for the execution, clearance, and settlement of Exchange transactions…unless it is protected against losses which might be incurred by members as a result of their use of such systems,'' and further that ''[t]o the extent [a limitation of liability rule] enables the Exchange to proceed with innovative systems, competition should be enhanced.''); Securities Exchange Act Release No. 58137 (July 10, 2008), 73 FR 41145 (July 17,

rules broadly disclaim all liability to exchange members. By way of example, NASDAQ Equities Rule 4626 provides that the exchange "shall not be liable for **any** losses, damages, or other claims arising out of the NASDAQ Market Center or its use."[17] Every other securities exchange has a similar rule, each of which was approved by the Commission as consistent with the Exchange Act.[18]

These Commission-approved limitations of liability support a foundational aspect of the Exchange Act: the self-regulatory framework. This bedrock principle of securities regulation dates back to 1934, when Congress initially codified the legal status of self-regulatory organizations.[19] The essence of this framework is that the Commission regulates the SROs, and, in turn, each SRO regulates its members.[20] To empower the self-regulatory organizations to regulate Industry Members, Congress granted the securities exchanges with the authority—and the responsibility—to enforce compliance with the securities laws among exchange members.[21]

2008) (SR–NYSE–2008–55) (explaining that exchange's limitation of liability rule encourages vendors to provide services to the exchange, which results in faster and more innovative products for order entry, execution, and dissemination of market information).

17 See Nasdaq Equities Rule 4626 (Limitation of Liability) (emphasis added).

18 New York Stock Exchange LLC Rule 17, BOX Exchange LLC, Rule 7230; Cboe Exchange, Inc., Rule 1.10; Investors Exchange LLC, Rule 11.260; Long-Term Stock Exchange, Rule 11.260; Miami International Securities Exchange, LLC, Rule 527; MEMX Rule 11.14. Although FINRA does not operate a securities exchange, the Commission has recognized that limiting FINRA's liability to Industry Members is consistent with the Exchange Act. *See* FINRA Rule 14108.

19 See Exchange Act Section 6(d).

20 Section 6 of Exchange Act requires the SROs to enact rules subject to SEC approval and enforce those rules against members. The Commission oversees the SROs through its examination authority under Section 17 and its enforcement authority pursuant to Sections 19(h)(1) and 21C.

21 See Exchange Act Section 6(b) (original version) (providing that exchanges must have provisions for expelling, suspending, or otherwise disciplining members for conduct that is inconsistent with just and equitable principles of trade and willful violations of the Exchange Act).

It is in this context that the Commission has concluded that rules requiring Industry Members to limit the liability of the Participants are consistent with the Exchange Act.

Likewise, the Commission has concluded that it is appropriate for self-regulatory organizations to adopt agreements with terms of use in connection with regulatory reporting facilities. The Commission has approved rules requiring Industry Members to agree to terms of use that customarily limit the liability of various regulatory reporting facilities—and the individual participants that comprise or operate those facilities—in connection with the reporting of order and execution data. And as with the CAT, those reporting facilities ingest substantial volumes of sensitive transaction data. For example, from 1998 through the present, the OATS has functioned as an integrated audit trail of order, quote, and trade data for equity securities. And to comply with their OATS reporting requirements, FINRA members must acknowledge an agreement that includes a limitation of liability provision that is similar in scope to the Limitation of Liability Provisions that are the subject of this Proposed Amendment.[22]

Congress and the Commission have recognized that these principles also apply to National Market System facilities comprised of self-regulatory organizations. In 1975, Congress enacted the Securities Act Amendments of 1975, which reinforced the importance of the self-regulatory framework. The 1975 legislation also tasked the exchanges with certain responsibilities for the creation of a "national market system" including the development and maintenance of a consolidated market data stream.[23]

---

22 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).

23 See Exchange Act Section 11A.

Following the adoption of the market data rules of Regulation NMS in 2007, various NMS facilities have been formed to execute the regulation's mandates. There too, the Commission has concluded that limitations of liability are consistent with the Exchange Act. Accordingly, NMS facilities that receive transaction and customer data uniformly contain broad limitations of liability protecting both the actual facility and its constituent self-regulatory organizations. For example, the Consolidated Quotation Plan vendor and subscriber agreements—approved by the Commission—provide that no disseminating party will:

> be liable in any way to [Customer/Subscriber] or to any other person for (a) any inaccuracy, error or delay in, or omission of, (i) any such data, information or message, or (ii) the transmission or delivery of any such data, information or message, or (b) any loss or damage arising from or occasioned by (i) any such inaccuracy, error, delay or omission, (ii) non-performance, or (iii) interruption in any such data, information or message, due either to any negligent act or omission by any Disseminating Party or to any "Force Majeure" (i.e., any flood, extraordinary weather conditions, earthquake or other act of God, fire, war, insurrection, riot, labor dispute, accident, action of government, communications or power failure, or equipment or software malfunction) or any other cause beyond the reasonable control of any Disseminating Party.[24]

---

[24] See Consolidated Tape Association/Consolidated Quotation Plan, July 1978, as restated December 1995 available at https://www.ctaplan.com/publicdocs/ctaplan/notifications/trader-update/CQ_Plan_-_9.17.2020.pdf. Other NMS facilities and regulatory reporting systems likewise require Industry Members to agree to limit the liability of SROs. The Commission has approved multiple NMS Plans and rules regarding reporting facilities that condition use of the facility on the execution of an agreement. See, e.g., Nasdaq Unlisted Trading Privileges Plan, available at http://www.utpplan.com/DOC/Nasdaq-UTPPlan_Composite_as_of_September_17_2020.pdf; Options Price Reporting Authority Plan, available at https://assets.website-files.com/5ba40927ac854d8c97bc92d7/5d0bd57d87d3ccca102102d7_OPRA%20Plan%20with%20Updated%20Exhibit%20A%20-%2006-19-2019.pdf. All such agreements limit liability. See, e.g., UTP Plan Subscriber Agreement, available at http://www.utpplan.com/DOC/subagreement.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.

As the Commission has recognized by approving limitations of liability in the rules of every self-regulatory organization and in the context of regulatory and NMS reporting facilities, limiting the liability of self-regulatory organizations to Industry Members is consistent with the Exchange Act. There is no reason to depart from the principles that served the securities markets well for over half of a century and create a different framework for CAT reporting. Indeed, to comply with the Administrative Procedure Act, the Commission may not depart from this longstanding approach without: (1) acknowledging the change in course and (2) providing a reasoned justification for the new, conflicting policy. See F.C.C. v. Fox Television Stations, Inc., 556 U.S. 502, 514-15 (2009). And because the Participants have invested substantial resources into the CAT in reliance on the agency's repeated approval of limitations on SRO liability, the Commission must provide an even more detailed justification if it opts to depart from that longstanding principle of liability here. See Smiley v. Citibank (South Dakota) N.A., 517 U.S. 735, 742 (1996) (explaining that "change that does not take account of legitimate reliance on prior interpretation … may be 'arbitrary, capricious, or an abuse of discretion") (citing 5 U.S.C. § 706(2)(A)); Fox Television Stations, Inc., 556 U.S. at 516 ("[A] reasoned explanation is needed for disregarding facts and circumstances that underlay or were engendered by the prior policy.").

The case for a limitation of liability is particularly compelling where, as here, the Participants and CAT LLC are implementing the requirements of the CAT NMS Plan in their regulatory capacities. Rule 613 of Regulation NMS tasked the SROs with creating 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."[25] During Rule 613's adoption, the Commission made clear that the rule imposed regulatory obligations on the Participants.[26] 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 securities self-regulatory organizations ("SROs") to perform their monitoring, enforcement, and regulatory activities more effectively."[27]

Notwithstanding the Commission's repeated conclusion that limiting the liability of the Participants and their facilities is consistent with the Exchange Act, during prior negotiations and during the Administrative Proceeding, SIFMA objected to *any* limitation of liability provision in the Reporter Agreement based on a purported "guiding principle" that the party that controls the data should bear the risk. But this "principle" is inapplicable to a regulatory program with Commission-mandated reporting.[28] It is also inconsistent with how SIFMA members treat their own customers. Despite controlling sensitive data that would harm customers if compromised via data breach, Industry Members routinely disclaim such liability.[29] At bottom, the

---

25 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.

26 SEC 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 20 (noting that prior to the CAT, SROs and the Commission must use a variety of data sources to fulfill their regulatory obligations).

27 August 17, 2010 SIFMA Letter at 1-2, available at https://www.sec.gov/comments/s7-11-10/s71110-63.pdf.

28 See, e.g., supra at 7, n. 21 (limitations of liability in regulatory reporting facilities).

29 See, e.g., Vanguard Electronic Services Agreement (effective Sep. 5, 2017), available at https://personal.vanguard.com/pdf/v718.pdf; E*TRADE Customer Agreement (effective June 30, 2020), available at https://us.etrade.com/e/t/estation/contexthelp?id=1209031000); Bank of America Electronic Trading Terms and Conditions (Nov. 2020), available at

Participants are not aware of any context in which liability that is usually borne by Industry Members is shifted to their regulators, and there is no compelling reason to do so here.

3. The Commission's Exemptive Relief Regarding PII Reduces the Risk of a Serious Data Breach

During negotiations regarding liability issues prior to the Administrative Proceeding, SIFMA focused on the allocation of liability between CAT LLC and Industry Members in the event of a data breach involving investors' personally identifiable information ("PII"). For example, SIFMA expressed concerns in correspondence dated November 11, 2019 that focused on inclusion of PII in the CAT, and in a similar letter dated January 8, 2020 expressed concerns about bulk downloading of data and PII.[30] The Participants appreciate those concerns and remain vigilant in taking all appropriate cybersecurity measures to protect customer information (and all CAT data). Further, the Commission subsequently 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.[31]

This plan amendment "minimizes the risk of theft of SSNs—the most sensitive piece of PII—by allowing the elimination of SSNs from the CAT, while still facilitating the creation of a reliable and accurate Customer-ID."[32] As discussed in detail by Charles River, and as the

---

https://www.bofaml.com/content/dam/boamlimages/documents/PDFs/baml_electronic_trading_platform_terms_final_12_03_2015.pdf).

30 In February 2020, SIFMA clarified that, in addition to PII concerns, a minority of Industry Members had refused to sign the Reporter Agreement due to concerns regarding the ability of third parties to reverse engineer their proprietary trading strategies.

31 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, SEC Release No. 34-88393 (Mar. 17, 2020).

32 Id. at 19.

Commission has recognized, the exemptive relief limiting customer information to phonebook data (i.e., name, address, and birth year) substantially minimizes the risk of a data breach involving sensitive customer data.[33] Due to this exemptive relief, 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.

4. The Proposed Limitation of Liability Provisions Are Necessary to Ensure the Financial Stability of the CAT

Limiting CAT LLC's and the Participants' liability in the event of a potential data breach is critical to ensuring a secure financial foundation for the CAT. 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."[34] To 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,[35] 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. Additionally, because the Commission has approved joint funding of CAT LLC by Industry Members and the Participants,[36] the Limitation of Liability Provisions also

---

33 Id. at 20 ("Reduction of these additional sensitive PII data elements in the CAT is expected to further reduce both the attractiveness of the database as a target for hackers and reduce the impact on retail investors in the event of an incident of unauthorized access and use."); Appendix B at 19, 21.

34 CAT NMS Plan § 11.2(f).

35 See infra at 13; See generally Appendix B.

36 See CAT NMS Plan at §§ 11.1-11.2. The Commission recently reiterated its support for the CAT NMS Plan's joint-funding model, and explicitly rejected the industry's argument that the Participants should not be permitted to recover fees, costs, and

protect the financial industry (and, in turn, the investing public) from the possibility of funding catastrophic losses.[37]

5. An Economic Analysis Highlights the Importance of Limiting CAT LLC's and the Participants' Liability

CAT LLC retained Charles River to conduct an economic analysis of liability issues in relation to a theoretical CAT data breach.[38] There are two principal components to this analysis. First, Charles River identified specific potential breach scenarios that could impact the CAT, and quantified the likelihood and potential financial magnitude of each scenario.[39] 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.[40]

Charles River's extensive economic analysis supports CAT LLC's and the Participants' decision to limit their liability to Industry Members. As detailed in the Charles River white paper (the "White Paper"), society can create incentives for economic actors—in this case, CAT

---

expenses from Industry Members. See May 15, 2020 Amendments to the National Market System Plan Governing the Consolidated Audit Trail, SEC Release No. 34-88890; File No. S7-13-19, at 39-40.

37 The CAT NMS Plan also mandates that the individual Participants shall not have any liability for any debts, liabilities, commitments, or any other obligations of CAT LLC or for any losses of CAT LLC. *See* CAT NMS Plan § 3.8(b). Accordingly, the Commission has authorized the substance of the Limitation of Liability Provisions as to self-regulatory organizations. Notably, SIFMA and its constituent Industry Members did not object to this provision of the CAT NMS Plan during the extensive notice and comment period for the CAT NMS Plan.

38 In the Administrative Proceeding, SIFMA asserted that "[t]he public has a significant interest in the allocation of risk (and resulting incentives) relating to a potential CAT data breach to ensure that data is not misused, misappropriated or lost." SIFMA Br. at 15. The Participants agree and asked Charles River to specifically assess whether a limitation of liability provision properly incentivizes all economic actors to take appropriate precautions against cyber incidents. *See* Appendix B at 1.

39 Appendix B at Section II.

40 Appendix B at Section III.

LLC, the Participants, and FINRA CAT—to take precautions to minimize the costs of accidents and misconduct. These incentives can take various forms, including: 1) enacting a regulatory regime that dictates specific ex ante rules that individuals and entities must follow, 2) asking courts to determine the appropriate standard of care ex post through litigation, or 3) a combination of both the regulatory and litigation approaches.[41] From an economic perspective, the choice between these methods is informed by the goal of maximizing social welfare—i.e., "the benefits [each] party derives from engaging in their activities, less the sum of the costs of precautions, the harms done, and the administrative expenses associated with the means of social control."[42] Charles River applied the well-settled body of economic literature regarding the respective benefits and costs of regulation and litigation, and concluded that allowing Industry Members to litigate against CAT LLC, the Participants, and FINRA CAT would provide minimal benefits while imposing substantial costs for all participants in the U.S. securities markets, including the Commission, Industry Members, the Participants, and the investing public. Under these circumstances, the economic analysis weighs heavily against permitting litigation and in favor of the Limitation of Liability Provisions.[43]

As discussed in the White Paper, a critical component of potential litigation benefits is the extent to which permitting Industry Members to litigate against CAT LLC and the Participants would incentivize CAT LLC and the Participants to appropriately invest in cybersecurity precautions.[44] Charles River addresses this question in the context of an extensive

---

41 Appendix B at 3.

42 Appendix B at 33 (citing Steven Shavell, "Liability for Harm Versus Regulation of Safety," The Journal of Legal Studies, Vol. 13, No.2 (June 1984), pp. 357-74).

43 Appendix B at 53-54.

44 Appendix B at 38.

regulatory regime that the Commission enacted to govern CAT LLC's and the Plan Processor's cybersecurity policies, procedures, systems, and controls.[45] After reviewing those measures from an economic perspective, Charles River concurs with the Commission's assessment "that the extensive, robust security requirements in the adopted Plan … provide appropriate, adequate protection for the CAT Data" and concludes that private litigation would not result in additional appropriate cybersecurity measures or produce other benefits.[46] In fact, as parties that use the CAT to carry out their own regulatory functions, the Participants have a strong incentive (beyond the obligation to comply with the Commission rules governing the CAT) to ensure that the CAT is secure and operational.

The Participants note that Charles River's analysis is borne out by their extensive discussions with Industry Members regarding the cybersecurity of the CAT and liability issues.[47] During negotiations with SIFMA prior to the launch of CAT reporting and the filing of the Administrative Proceeding, the Participants repeatedly asked SIFMA to identify specific deficiencies in the CAT's cybersecurity program. SIFMA was unable to do so, which is not surprising in light of CAT's robust cybersecurity.[48] To the extent that Industry Members

---

45 Appendix B at 3.

46 Order Approving the NMS Plan Governing the CAT, Section V.F.4, p. 715; Appendix B at 3, 54.

47 As part of the Participants' efforts to give SIFMA and its members further comfort as to the security of the CAT system, and as suggested by the Commission, the Participants have offered to facilitate a meeting with security officials from the SROs and the Industry Members to discuss the CAT's extensive cybersecurity and respond to questions that might constructively address SIFMA's concerns. The Participants remain willing to facilitate this meeting and look forward to opportunities to foster an open dialogue regarding security issues with Industry Members.

48 See, e.g., CAT NMS Plan, Section 6.6 (noting requirement that CAT LLC evaluate its information security program "to ensure that the program is consistent with the highest industry standards for the protection of data").

conclude that CAT LLC should make adjustments to its policies, procedures, systems, and controls, Industry Members (and other constituencies) have extensive avenues to provide feedback including through the Advisory Committee or by directly petitioning the Commission to amend the CAT NMS Plan.[49] Industry Members' inability to identify any meaningful deficiencies underscores Charles River's conclusion that CAT LLC is already properly incentivized to take necessary cyber precautions. Allowing Industry Members to litigate against CAT LLC and the Participants would not further improve the CAT's cybersecurity or produce any other programmatic benefits.[50]

Charles River's analysis also highlights that, as heavily regulated entities, CAT LLC and the Participants have a strong incentive to comply with the Commission's rules—i.e., another advantage of the ex-ante regulatory regime already in place.[51] Moreover, as Charles River notes, regulatory systems are particularly appropriate where, as here, the regulator (i.e., the Commission) is enacting rules that are designed to govern one entity (i.e., CAT LLC).[52] As a result, "the regulatory system is tailored specifically on an ex-ante basis with rules targeted to

---

49 As Charles River highlights, the sufficiency of the regulatory regime here is underscored by the ability of the Commission—whether in response to concerns from Industry Members or on its own initiative—to revise the applicable rules to impose additional cybersecurity measures on CAT LLC, the Plan Processor, and the Participants. *See* Appendix B at 43. The Commission has not hesitated to propose revisions when necessary, including, most recently in August 2020. *See* SEC Release No. 34-89632; File No. S7-10-20, Proposed Amendments to the National Market System Plan Governing the Consolidated Audit Trail to Enhance Data Security (Aug. 21, 2020).

50 Appendix B at 54.

51 Appendix B at 39. It is also worth noting that 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." SEC Release No. 34-89632; File No. S7-10-20, Proposed Amendments to the National Market System Plan Governing the Consolidated Audit Trail to Enhance Data Security (Aug. 21, 2020), at 9.

52 Appendix B at 3-4, 43.

this particular firm."[53] As part of the regulatory regime, CAT LLC's cybersecurity policies, procedures, systems, and controls are subject to examination by the Office of Compliance Inspections and Examinations (on both a for-cause and cyclical basis).[54] And any cybersecurity deficiencies could, of course, be referred to the Division of Enforcement for an investigation and potential enforcement action.[55] As Charles River notes, this regulatory enforcement structure creates strong incentives for CAT LLC and the Participants to comply with the Commission's extensive cyber regulatory regime.[56]

In assessing the value of permitting Industry Members to sue CAT LLC and the Participants, an economic analysis also must consider the costs of litigation. Charles River's White Paper addresses this question and concludes that the costs of litigating a potential CAT data breach are likely to be both substantial and unquantifiable on an ex-ante basis.[57] 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 who would ultimately pass those higher costs on to their customers, employees or owners."[58] Critically, these added costs—whether resulting from litigation, investment in cybersecurity beyond optimal levels, or any other

53 Appendix B at 43.

54 Appendix B at 43.

55 Appendix B at 3, 37.

56 Appendix B at 3-4, 43.

57 Appendix B at 46.

58 Appendix B at 46.

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."[59] The White Paper also explains that excess cybersecurity measures driven by third-party litigation risk could reduce the CAT's effectiveness in serving the Commission's and the SROs' regulatory missions, and likewise could result in court-ordered security measures that conflict or interfere with the security regime adopted by the Commission.[60] The combination here of no articulable benefit of allowing litigation coupled with costs that are potentially "substantial" and "unquantifiable" present the quintessential economic case in favor of a limitation of liability.

Charles River's analysis of potential breach scenarios further supports the need for CAT LLC, the Participants, and FINRA CAT to limit their liability to Industry Members. Charles River identified eight potential scenarios in which a bad actor could unlawfully obtain, utilize, and monetize CAT data.[61] The analysis indicates 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.[62] Charles River's review supports the Commission's conclusion that CAT LLC's cybersecurity program provides "appropriate, adequate protection for the CAT Data."[63] The Participants know of no valid basis for challenging that Commission finding.

---

59 Appendix B at 47. The Commission has a statutory obligation to consider efficiency, competition, and effects on capital formation when engaging in rulemaking. *See* 15 U.S.C. 77b(b); 15 U.S.C. 78c(f); 15 U.S.C. 80a-2(c).

60 Appendix B at 45.

61 Appendix B at 2, 18-32.

62 Appendix B at 18-32.

63 Order Approving the NMS Plan Governing the CAT, Section V.F.4, p. 715.

During the negotiations prior to the Administrative Proceeding, SIFMA focused extensively on the possibility of a hacker reverse engineering certain Industry Members' proprietary trading strategies. In that regard, Charles River's scenario analysis indicates that reverse engineering of trading algorithms—and two other potential breach scenarios—could result in "extremely" severe economic consequences (i.e., potentially greater than $100 million in damages).[64] In light of CAT LLC's cybersecurity and the attendant difficulties that a bad actor would face in monetizing these scenarios, Charles River concluded that all three of these potential categories of breaches (including reverse engineering of trading algorithms) are relatively low-frequency events.[65]

Even if these low probability scenarios occurred, there is no economic basis for shifting liability for potential catastrophic losses to CAT LLC or the Participants.[66] Indeed, if CAT LLC or the Participants could be required to fund such substantial losses, it would need to be reflected in the funding structure for the CAT, and the portion of the losses that is funded by the Participants would effectively be passed on to all market participants, including retail investors. Shifting liability to CAT LLC or the Participants is fundamentally inconsistent with the Commission's longstanding views on allocation of liability between self-regulatory organizations and Industry Members memorialized in the Commission-approved rules of every

64 Appendix B at 2.

65 Appendix B at 25. As Charles River explains, while "[w]e ultimately deem it unlikely that a bad actor would seek to use CAT data in this way because of the difficulty in both achieving the hack as well as the effort to reverse engineer an algorithm, … [g]iven the potential value (severity) of this type of information, however, bad actors could be so motivated."

66 Appendix B at 50.

securities exchange, and in agreements for NMS facilities, as well as regulatory reporting facilities.[67]

B. Governing or Constituent Documents

Not applicable.

C. Implementation of Amendment

The Participants propose to implement the Limitation of Liability Provisions by requiring all CAT Reporters and CAT Reporting Agents to execute revised agreements that contain the amended provisions.

D. Development and Implementation Phases

The Participants propose to require CAT Reporters and CAT Reporting Agents to execute the revised agreements upon Commission approval of this Proposed Amendment.

E. Analysis of Impact on Competition

The Participants do not believe the Proposed Amendment will have any impact on competition. The Proposed Amendment would require all CAT Reporters and CAT Reporting Agents to execute revised agreements that contain the amended provisions. Adopting the Proposed Amendment would, however, avoid the increased costs that would otherwise arise, and therefore would promote efficiency and capital formation in the U.S. securities markets. Indeed, the 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 third-party litigation) would generate few, if any, benefits while imposing significant costs.[68]

---

67 See supra at Section A3.

68 See Appendix B at Sections III(A)-(D).

F. Written Understanding or Agreements Relating to Interpretation of, or Participation in, Plan

Not applicable.

G. Approval by Plan Sponsors in Accordance with Plan

Section 12.3 of the CAT NMS Plan states that, subject to certain exceptions, the Plan may be amended from time to time only by a written amendment, authorized by the affirmative vote of not less than two-thirds of all of the Participants, that has been approved by the SEC pursuant to Rule 608 or has otherwise become effective under Rule 608. The Participants, by a vote of the Operating Committee taken on December 15, 2020 have authorized the filing of this Proposed Amendment with the SEC in accordance with the Plan.[69]

H. Description of Operation of Facility Contemplated by the Proposed Amendment and any Fees or Charges in Connection thereto

Not applicable.

I. Terms and Conditions of Access

Any CAT Reporter or CAT Reporting Agent that fails to execute a revised agreement with the Limitation of Liability Provisions will not be permitted to transmit data to the CAT. Pursuant to the court's decision in NASDAQ Stock Market, LLC v. SEC, 961 F.3d 421 (D.C. Cir. 2020), this restriction will not constitute a denial of access to services within the meaning of Section 19(d) of the Exchange Act.

J. Method and Frequency of Processor Evaluation

Not applicable.

---

69 The Participants remain willing to work with SIFMA in good faith to resolve any remaining differing perspectives on liability. Although we believe that the Limitation of Liability Provisions in Appendix A are appropriate, we look forward to constructively engaging with SIFMA during the comment process to address any concerns that Industry Members may have.

K. Dispute Resolution

Not applicable.

III. Solicitation of Comments

Interested persons are invited to submit written data, views and arguments concerning the foregoing, including whether the amendment is consistent with the Exchange Act. Comments may be submitted by any of the following methods:

Electronic Comments:

- Use the Commission's Internet comment form (http://www.sec.gov/rules/sro.shtml); or
- Send an e-mail to rule-comments@sec.gov. Please include File Number 4-698 on the subject line.

Paper Comments:

- Send paper comments to Secretary, Securities and Exchange Commission, 100 F Street, NE, Washington, DC 20549-1090.

All submissions should refer to File Number 4-698. This file number should be included on the subject line if e-mail is used. To help the Commission process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission's Internet website (http://www.sec.gov/rules/sro.shtml). Copies of the submission, all subsequent amendments, all written statements with respect to the proposed plan amendment that are filed with the Commission, and all written communications relating to the amendment between the Commission and any person, other than those that may be withheld from the public in accordance with the provisions of 5 U.S.C. 552, will be available for website viewing and printing in the Commission's Public Reference Room, 100 F Street, NE, Washington, DC 20549, on official business days between the hours of 10:00 am and 3:00 pm. Copies of such filing also will be available for inspection and copying at the Participants' offices. All comments received

will be posted without change. Persons submitting comments are cautioned that we do not redact or edit personal identifying information from comment submissions. You should submit only information that you wish to make available publicly. All submissions should refer to File Number 4-698 and should be submitted on or before [insert date 21 days from publication in the Federal Register].

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.[70]

J. Matthew DeLesDernier
Assistant Secretary

[70] 17 CFR 200.30-3(a)(85).

APPENDIX A

LIMITED LIABILITY COMPANY AGREEMENT OF CONSOLIDATED AUDIT TRAIL, LLC

* * * * *

ARTICLE XII

[proposed additions]

* * * * *

Section 12.15. Limitation of Liability. Each CAT Reporter shall be required to execute an amended Consolidated Audit Trail Reporter Agreement containing, in substance, the limitation of liability provisions in Appendix E to this Agreement. Each Person engaged by a CAT Reporter to report CAT Data to the Central Repository on behalf of such CAT Reporter shall be required to execute an amended Consolidated Audit Trail Reporting Agent Agreement containing, in substance, the limitation of liability provisions in Appendix F to this Agreement. The Operating Committee shall have authority in its sole discretion to make non-substantive amendments to the limitation of liability provisions in the Consolidated Audit Trail Reporter Agreement and the Consolidated Audit Trail Reporting Agent Agreement.

* * * * *

APPENDIX E

[proposed additions]

* * * * *

Limitation of Liability Provisions in the CAT Reporter Agreement

5.4. Disclaimer. EXCEPT AS EXPRESSLY SET FORTH IN SECTION 5.1 OF THIS AGREEMENT, CATLLC MAKES NO REPRESENTATIONS OR WARRANTIES, ORAL OR WRITTEN, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, QUALITY, FITNESS FOR A PARTICULAR PURPOSE, COMPLIANCE WITH APPLICABLE LAWS, NON-INFRINGEMENT OR TITLE, SEQUENCING, TIMELINESS, ACCURACY OR COMPLETENESS OF INFORMATION, OR THOSE ARISING BY STATUTE OR OTHERWISE IN LAW, OR FROM A COURSE OF DEALING OR USAGE OF TRADE, REGARDING THE CAT SYSTEM OR ANY OTHER MATTER PERTAINING TO THIS AGREEMENT. CAT REPORTER ACCEPTS SOLE RESPONSIBILITY FOR ITS ACCESS TO AND USE OF THE CAT SYSTEM.

5.5. Limitation of Liability. TO THE EXTENT PERMITTED BY LAW, UNDER NO CIRCUMSTANCES SHALL THE TOTAL LIABILITY OF CATLLC OR ANY OF ITS REPRESENTATIVES TO CAT REPORTER UNDER THIS AGREEMENT FOR ANY CALENDAR YEAR EXCEED THE LESSER OF THE TOTAL OF THE FEES ACTUALLY

PAID BY CAT REPORTER TO CATLLC FOR THE CALENDAR YEAR IN WHICH THE CLAIM AROSE OR FIVE HUNDRED DOLLARS ($500.00). FOR AVOIDANCE OF DOUBT, THE TERM "REPRESENTATIVES" IN SECTION 5 AND THROUGHOUT THIS AGREEMENT SHALL INCLUDE 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.

5.6. Damage Exclusion. TO THE EXTENT PERMITTED BY LAW, UNDER NO CIRCUMSTANCES SHALL CATLLC OR ANY OF ITS REPRESENTATIVES BE LIABLE TO CAT REPORTER OR ANY OTHER PERSON FOR LOST REVENUES, LOST PROFITS, LOSS OF BUSINESS, OR ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY, PUNITIVE OR OTHER DIRECT OR INDIRECT DAMAGES OF ANY KIND OR NATURE, INCLUDING, SUCH DAMAGES ARISING FROM ANY BREACH OF THIS AGREEMENT, OR ANY TERMINATION OF THIS AGREEMENT, WHETHER SUCH LIABILITY IS ASSERTED ON THE BASIS OF CONTRACT, TORT OR OTHERWISE, WHETHER OR NOT FORESEEABLE, EVEN IF CAT REPORTER OR ANY OTHER PERSON HAS BEEN ADVISED OR WAS AWARE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES.

5.7. Data Exclusion. TO THE EXTENT PERMITTED BY LAW, UNDER NO CIRCUMSTANCES SHALL CATLLC OR ANY OF ITS REPRESENTATIVES BE LIABLE FOR ANY INCONVENIENCE CAUSED BY THE LOSS OF ANY DATA, FOR THE LOSS OR CORRUPTION OF ANY CAT REPORTER DATA OR FOR ANY DELAYS OR INTERRUPTIONS IN THE OPERATION OF THE CAT SYSTEM FROM ANY CAUSE.

* * * * *

APPENDIX F

[proposed additions]

* * * * *

Limitation of Liability Provisions in the CAT Reporting Agent Agreement

5.4 Disclaimer. EXCEPT AS EXPRESSLY SET FORTH IN SECTION 5.1 OF THIS AGREEMENT, CATLLC MAKES NO REPRESENTATIONS OR WARRANTIES, ORAL OR WRITTEN, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, QUALITY, FITNESS FOR A PARTICULAR PURPOSE, COMPLIANCE WITH APPLICABLE LAWS, NON-INFRINGEMENT OR TITLE, SEQUENCING, TIMELINESS, ACCURACY OR COMPLETENESS OF INFORMATION, OR THOSE ARISING BY STATUTE OR OTHERWISE IN LAW, OR FROM A COURSE OF DEALING OR USAGE OF TRADE, REGARDING THE CAT SYSTEM OR ANY OTHER MATTER PERTAINING TO THIS AGREEMENT. CAT REPORTING AGENT ACCEPTS SOLE RESPONSIBILITY FOR ITS ACCESS TO AND USE OF THE CAT SYSTEM.

5.5 Limitation of Liability. TO THE EXTENT PERMITTED BY LAW, UNDER NO CIRCUMSTANCES SHALL THE TOTAL LIABILITY OF CATLLC OR ANY OF ITS REPRESENTATIVES TO CAT REPORTING AGENT UNDER THIS AGREEMENT FOR ANY CALENDAR YEAR EXCEED THE LESSER OF THE TOTAL OF THE FEES ACTUALLY PAID TO CATLLC BY THE CAT REPORTER THAT ENGAGED CAT REPORTING AGENT FOR THE CALENDAR YEAR IN WHICH THE CLAIM AROSE OR FIVE HUNDRED DOLLARS ($500.00). FOR AVOIDANCE OF DOUBT, THE TERM "REPRESENTATIVES" IN SECTION 5 AND THROUGHOUT THIS AGREEMENT SHALL INCLUDE 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.

5.6 Damage Exclusion. TO THE EXTENT PERMITTED BY LAW, UNDER NO CIRCUMSTANCES SHALL CATLLC OR ANY OF ITS REPRESENTATIVES BE LIABLE TO CAT REPORTING AGENT OR ANY OTHER PERSON FOR LOST REVENUES, LOST PROFITS, LOSS OF BUSINESS, OR ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY, PUNITIVE OR OTHER DIRECT OR INDIRECT DAMAGES OF ANY KIND OR NATURE, INCLUDING, SUCH DAMAGES ARISING FROM ANY BREACH OF THIS AGREEMENT, OR ANY TERMINATION OF THIS AGREEMENT, WHETHER SUCH LIABILITY IS ASSERTED ON THE BASIS OF CONTRACT, TORT OR OTHERWISE, WHETHER OR NOT FORESEEABLE, EVEN IF CAT REPORTING AGENT OR ANY OTHER PERSON HAS BEEN ADVISED OR WAS AWARE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES.

5.7 Data Exclusion. TO THE EXTENT PERMITTED BY LAW, UNDER NO CIRCUMSTANCES SHALL CATLLC OR ANY OF ITS REPRESENTATIVES BE LIABLE FOR ANY INCONVENIENCE CAUSED BY THE LOSS OF ANY DATA, FOR THE LOSS OR CORRUPTION OF ANY DATA SUBMITTED BY CAT REPORTING AGENT OR FOR ANY DELAYS OR INTERRUPTIONS IN THE OPERATION OF THE CAT SYSTEM FROM ANY CAUSE.

* * * * *

Appendix B

White Paper:

Analysis of Economic Issues Attending the Cyber Security of the Consolidated Audit Trail

Date: December 18, 2020

Table of Contents

I. Introduction

II. Cyber Security Risk Analysis

- A. Overall Cost of Cybercrime
- B. Parties Harmed by Cybercrime
- C. Types of Bad Actors, Motivations, and Methods
- D. Cyber Breaches Relevant to CAT, LLC Including Frequency, Severity, and Relative Difficulty of Implementation
  1. Summary Level Data
  2. Breach Data Specifically Relevant to CAT, LLC
- E. Summary

III. Economic and Public Policy Analysis of Cyber Security for CAT LLC

- A. The Choice Between Regulation and Litigation
- B. Economic Determinants of the Relative Attractiveness of Regulation or Litigation to Control Risk
- C. Special Considerations Arising for the CAT's Cyber Security
- D. Assessment of Regulation and Litigation Approaches as Applied to a Potential CAT LLC Cyber Breach
  1. Recapitulation of CAT's Risks, Standards, Policies, and Practices
  2. Alignment of Incentives
  3. Additional Costs of Litigation
  4. Examples of Existing Limitation on Liability Provisions
- E. Initial Thoughts on Funding Compensation Mechanisms

IV. Conclusion

V. Qualifications of Authors / Investigators

VI. Research Program and Bibliography

I. Introduction

Charles River Associates ("CRA")[1] has been asked by a group of national securities exchanges[2] and the Financial Industry Regulatory Authority, Inc. ("FINRA") (collectively "Participants" or "SROs") to assess the economic aspects of a potential cyber breach as a result of the operation of the Consolidated Audit Trail ("CAT"). The CAT is being implemented by the Participants in response to Rule 613, which the SEC adopted in 2012. Rule 613 was adopted to improve the regulation of U.S. equity and option markets by requiring the collection, storage, and access to a wide range of equity and option transactions and orders. The CAT exists so that the SEC and the SROs can more effectively monitor and regulate the subject securities markets to improve their transparency, robustness, and efficiency for the benefit of the investing public and capital markets as a whole.

The Participants and the securities industry agree that the CAT database contains sensitive information and the SEC has mandated extensive security requirements be implemented to protect the data from a wide range of cyber breaches. After considering the overall costs and benefits of the CAT, the SEC already has concluded that the cyber security requirements it imposed on the CAT sufficiently serve the public interest.[3]

---

1 The identification and qualifications of CRA's authors / principal investigators for this White Paper are presented in Section V below.

2 As of January 2020, these consisted of: (1) BOX Exchange LLC, (2) Cboe BYX Exchange, Inc., (3) Cboe BZX Exchange, Inc., (4) Cboe EDGA Exchange, Inc., (5) Cboe EDGX Exchange, Inc., (6) Cboe C2 Exchange, Inc., (7) Cboe Exchange, Inc., (8) Investors Exchange LLC, (9) Long Term Stock Exchange, Inc., (10) Miami International Securities Exchange LLC, (11) MIAX Emerald, LLC, (12) MIAX PEARL, LLC, (13) NASDAQ BX, Inc., (14) Nasdaq GEMX, LLC, (15) Nasdaq ISE, LLC, (16) Nasdaq MRX, LLC, (17) NASDAQ PHLX LLC, (18) The NASDAQ Stock Market LLC, (19) New York Stock Exchange LLC, (20) NYSE American LLC, (21) NYSE Arca, Inc., (22) NYSE Chicago, Inc., and (23) NYSE National, Inc. In addition, a new member-owned equities trading platform, Members Exchange ("MEMX LLC") launched in September 2020. These entities plus FINRA have been designated as "Participants" of the CAT NMS Plan and are self-regulatory organizations ("SROs") under the Securities Exchange Act of 1934. See Securities and Exchange Commission, *Order Granting Conditional Exemptive Relief, Pursuant to Section 36 and Rule 608(e) of the Securities Exchange Act of 1934, from Section 6.4(d)(ii)(C) and Appendix D Sections 4.1.6, 6.2, 8.1.1, 8.2, 9.1, 9.2, 9.4, 10.1, and 10.3 of the National Market System Plan Governing the Consolidated Audit Trail,* Release No. 34-88393, March 17, 2020, p. 1, hereafter "SEC, *March 17, 2020 Order*."

3 Securities and Exchange Commission, *Joint Industry Plan; Order Approving the National Market System Plan Governing the Consolidated Audit Trail,* Release No. 34-79318, November 15, 2016, hereafter "SEC, *Order Approving CAT*," Section IV. Discussion and Commission Findings, pp. 126-127.

The analyses presented in this paper support the Participants' proposal to adopt a limitation of liability provision in the CAT Reporter Agreement. Based on (1) an examination of specific potential breach scenarios and (2) a consideration of the economic and public policy elements of various regulatory and litigation approaches to mitigate cyber risk for the CAT, this paper concludes that a limitation on liability provision would serve the public interest in several ways. *First*, such a provision would facilitate the regulation of the U.S. equity and option markets at lower overall costs and higher economic efficacy than other approaches, such as allowing Industry Members[4] to litigate against CAT LLC. *Second*, the proposed limitation on liability would not undermine CAT LLC's existing and significant incentives to protect the data stored in the CAT system.

Summary: Cyber Breach Analysis. The first analysis we present is to identify specific potential breach scenarios and assess the relative difficulty of implementation, relative frequency, and conditional severity of each. As part of this assessment, we identified eight potential scenarios in which bad actors could attempt to unlawfully obtain, utilize, and monetize CAT data. Of course, we recognize that cyber-attacks on the CAT could vary from the scenarios we hypothesize, but we offer them to provide a framework to assess the economic exposures that flow from the gathering, storage, and use of CAT data. Our risk analysis indicates that most of these scenarios are relatively low frequency events because they are either difficult to implement, unlikely to be meaningfully profitable for a bad actor, or both.

The scenario analysis also indicates that three types of breaches—reverse engineering of trading algorithms, inserting fake data to wrongfully incriminate individuals or entities, and removing data to conceal misconduct—could result in "extremely" severe economic consequences (which we define as potentially greater than $100 million in damages). We conclude that all three of these types of breaches are relatively low frequency events.

Summary: Regulation vs. Litigation to Mitigate Cyber Risk for the CAT. The second analysis we present focuses on whether the cyber risk posed by CAT should be addressed through *ex-ante* regulation, *ex post* litigation, or a combination of both approaches. In a prior version of the CAT Reporter Agreement, CAT LLC included a limitation of liability provision, which memorialized the Participants' view that Industry Members should not be able to litigate against CAT LLC or the Participants to recover damages sustained as a result of a cyber breach. Although the current operative version of the Reporter Agreement does not contain a limitation of liability, we understand that CAT LLC is submitting this White Paper in connection with CAT LLC's request that the SEC amend the CAT NMS Plan to authorize such a provision. We understand that the Industry Members have opposed any limitation of liability provision and

---

[4] "Industry Member" is defined as, "a member of a national securities exchange or a member of a national securities association" in the "Limited Liability Company Agreement of CAT NMS, LLC," p.5. The Securities Industry and Financial Markets Association ("SIFMA") has represented their interests in this SEC rule-making endeavor.

contend that CAT LLC, as the party holding the CAT data, should be subject to litigation by the Industry Members in the event of a cyber breach.

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. As part of our analysis, we specifically assess whether including a limitation of liability provision in the CAT Reporter Agreement is appropriate from the perspective of economic theory as applied to the specifics of this situation.

By applying the economic principles of liability and regulation as a means of motivating risk-minimizing behavior and considering the crucial role of the SEC's mandates regarding cyber security for the CAT (which already incorporate the concerns of entities involved in the National Market System as a whole), we conclude that the regulatory approach leads to the socially desirable level of investment in cyber security and protection of CAT data. We further conclude that SIFMA's position, which advocates allowing Industry Members to litigate against CAT LLC and the Participants in the event of a cyber breach, would result in increased costs for various economic actors—including CAT LLC, the Participants, Industry Members, and retail investors—without any meaningful benefit to the CAT's cyber security. At a high level (and as discussed in extensive detail below), we therefore conclude that CAT LLC's proposal to limit its liability and the liability of the Participants is well supported by applicable economic principles in the framework of the SEC's mission and its mandates regarding the CAT.

As a general matter, economic theory provides that society can motivate economic actors to take appropriate precautions to minimize the likelihood and consequences of accidents and misconduct through: a) a regulatory approach (i.e., dictating specific precautions, requirements, and standards in advance), b) a litigation approach (i.e., civil liability for damages caused by failing to adhere to a general standard of care), or c) a combination of (a) and (b). At the outset, we note that we do not address this question in a vacuum. Rather, we conduct our examination in the context of an extensive regulatory program that the SEC has enacted mandating specific cyber standards, policies, procedures, systems, and controls that CAT LLC and the Plan Processor must implement. This regulatory regime was developed with extensive feedback from the securities industry (e.g., through the Development Advisory Group and the Advisory Committee) and is subject to ongoing review and modification through a public review and comment process. Moreover, CAT LLC's compliance with the requirements of this regulatory regime can be policed by the SEC's Enforcement Division. We also note that in adopting the CAT NMS Plan, the SEC concluded that the regulatory approach to cyber security was sufficient when it stated that "the extensive, robust security requirements in the adopted [CAT NMS] Plan … provide appropriate, adequate protection for the CAT Data."[5]

---

[5] SEC, *Order Approving CAT,* Section V.F.4. *Economic Analysis, Expected Costs of Security Breaches,* p. 715.

In light of this existing regulatory regime, the relevant question is whether the benefits of allowing Industry Members to litigate against their regulators in the event of a CAT data breach outweigh the costs. An application of economic principles indicates that they do not. As heavily regulated entities, the Participants are obligated to comply with all SEC requirements and maintain an effective cyber security program. And to the extent that CAT LLC and the Participants fail to comply with the SEC's regulatory regime, the SEC could compel compliance by bringing enforcement actions. Moreover, regulatory systems are particularly appropriate where, as here, the regulator (i.e., the Commission) is enacting rules that are designed to govern one entity (i.e., CAT LLC). Further, the SEC's regulatory process for the CAT permits parties affected by the operation of the CAT to stay informed of the operation of the CAT's cyber risk program and to advocate for and incorporate any broader security concerns that may arise. Indeed, there already exist examples where Industry Members have exercised these rights and successfully sought changes in the CAT's cyber security program. Under these circumstances, allowing Industry Members to further litigate against the Participants for damages resulting from cyber breaches would not better align the incentives or meaningfully increase the motivation of CAT LLC, the Plan Processor, or the Participants to pursue additional economically appropriate measures to reduce the frequency and severity of cyber breaches. Allowing these lawsuits would, however, increase costs to the Participants and Industry Members, much of which would be passed on to underlying investors. Where, as here, the costs of adding a litigation regime to an existing regulatory regime are high, and the expected benefits are low, there is no economic justification for allowing additional litigation.

It is also important to note that the CAT has no paying customers and is fully funded by Participants and Industry Members who, ultimately, pass those costs on to the investing public. CAT LLC's funding is designed to cover costs only, and its balance sheet is not intended to develop and hold assets available to compensate Industry Members or others who may be harmed in the event of a cyber breach.

We conclude, therefore, that the risk presented by a cyber breach of the CAT should be addressed through the regulatory approach that the SEC has already adopted. The limitation of liability provision in CAT LLC's proposed amended Reporter Agreement is therefore appropriate. In this regard, we note that limitations of liability are ubiquitous in the securities industry and have effectively governed the economic relationships between the Participants and Industry Members for decades. We also observe that although SIFMA has objected to a limitation of liability on behalf of Industry Members, Industry Members generally require their respective customers—many of whom are retail investors—to agree to analogous limitation of liability provisions.

An unfortunate fact of the cyber world is that the best standards, policies, and procedures all executed with perfection may not thwart every conceivable breach attempt. A successful cyber-attack on the CAT could result in injury to Industry Members. Even in a purely regulated regime, it is appropriate to consider mechanisms that provide compensation to parties injured by a cyber-attack on the regulated activity. It is worth noting that CAT LLC and the Plan Processer purchase insurance designed to provide compensation to harmed parties, up to pre-defined

economically feasible limits. The cyber insurance program also provides the benefit of engaging additional third parties (i.e., the insurance carriers) who have incentives and abilities to monitor cyber security hygiene at the CAT and the Plan Processor.

CAT LLC, the Participants, and the SEC could consider additional mechanisms beyond cyber insurance to compensate potentially harmed parties, including mechanisms similar to those used by federal vaccine programs or insolvency protections for pension funds or financial institutions. However, a careful evaluation of the costs, benefits, and incentives among the various parties associated with the CAT would need to be conducted to ensure that any new arrangement enhances economic welfare before any decision to further extend the current compensation scheme (i.e., CAT LLC's insurance) is made.

Section II below examines a list of potential cyber threats, identifies those that may apply to the CAT, and provides an initial quantification of the harms that may befall the CAT and others should a cyber threat be successful. Section III addresses the economic theory behind liability assignment and the roles that markets, contracts, litigation, and regulation play. It highlights the duplicative and overall cost-raising nature of the Industry Members' litigation proposal. It explains how the SEC's regulatory approach along with the efforts of the CAT, the Plan Processor, and the Advisory Committee, work to align the incentives of the CAT and the Plan Processor to mitigate the cyber risks and ensure the fairness of the Participants' proposed limitation on liability. Section IV contains some concluding comments. Section V presents the qualifications of the authors / principal investigators of this White Paper. Section VI summarizes the research undertaken for this White Paper and contains the bibliography.

II. Cyber Security Risk Analysis

In this section we discuss the economic risk associated with bad actors wrongfully accessing the CAT system to monetize the data or to disrupt market surveillance. The CAT will store massive quantities of data that is unavailable anywhere else on a single system, which as Commissioner Pierce recently recognized, will "undoubtedly" be a target for hackers.[6] The CAT is the only data repository that collects and holds Customer and Customer Account Information[7]

---

6 Commissioner Pierce Statement on Proposed Amendments to the National Market System Plan Governing the Consolidated Audit Trail to Enhance Data Security, Aug. 21, 2020, https://www.sec.gov/news/public-statement/peirce-nms-cat-2020-08-21 accessed September 2020.

7 The SEC proposes to "delete the term "PII" from the CAT NMS Plan and replace that term with "Customer and Account Attributes" as that would more accurately describe the attributes that must be reported to the CAT, now that ITINs/SSNs, dates of birth and account numbers would no longer be required to be reported to the CAT pursuant to the amendments being proposed by the Commission." Additionally, the SEC proposes to delete the defined term "PII" from the CAT NMS Plan given the reporting of the most sensitive PII will no longer be required. The SEC proposes that "Customer and Account Attributes" refer collectively to all the attributes in "Customer Attributes" and "Account Attributes." The SEC proposes that "Customer Attributes" would include name, address, year of birth, the individual's role in the account or if a legal entity, the name, address,

along with all trading data from the participating U.S. securities exchanges.[8] The compromise of this data, as discussed in further detail below, could harm broker/dealers, and exchanges, or undermine investor confidence in the markets themselves.

Given the importance of the CAT data, there are a variety of cyber security breach scenarios that, hypothetically, could occur and harm the CAT, the Plan Processor, the Participants, Industry Members, the investing public, the SEC's ability to surveil activity in the markets, and (conceivably) the functioning of U.S. securities markets.

Below, we posit a range of potential cyber risk scenarios attendant to the CAT and derive estimated ranges of potential financial consequences arising from these exposures. We recognize cyber attacks on the CAT could vary from the scenarios we hypothesize, but we offer them to provide a framework to assess the economic exposures that flow from the gathering of a massive amount of sensitive trading, financial, and identifying data. Some of the scenarios present relatively small economic risk, while others present significant risk in terms of both financial consequence and the potential to undermine faith in the efficiency and fairness of U.S. markets.

Overall, this section is organized as follows:

A. Overall Cost of Cybercrime

B. Parties Harmed by Cybercrime

C. Types of Bad Actors, Motivations, and Methods

D. Cyber Breaches Relevant to CAT, LLC Including Relative Difficulty of Implementation, Frequency and Severity

E. Summary

A. Overall Cost of Cybercrime

"Cybercrime is a growth industry" and "produces high returns at low risk and (relatively) low cost for the hackers."[9]

Estimates of the worldwide cost of cybercrime are in the trillions of dollars per year and continuing to grow.

---

and Employer Identification Number and Legal Entity Identifier. The SEC proposes that "Account Attributes" would include account type, customer type, date account opened, and large trader identifier (if applicable). Securities and Exchange Commission, *Amendments to the National Market System Plan Governing the Consolidated Audit Trail to Enhance Data Security,* RIN 3235-AM62, Release No. 34-89632, File No. S7-10-20, August 21, 2020, pp. 103-106.

8 See SEC website, "Rule 613 (Consolidated Audit Trail)," https://www.sec.gov/divisions/marketreg/rule613-info.htm accessed September 2020.

9 The Center for Strategic and International Studies, "Net Losses: Estimating the Global Cost of Cybercrime," June 2014, pp. 2 and 4.

(a) $3 trillion per year in 2015 and $6 trillion annually by 2021 according to Cybersecurity Ventures.[10]

(b) $3 trillion per year in 2019 to $5 trillion by 2024 according to Juniper Research.[11]

In the United States, according to the Council of Economic Advisers, malicious cybercrime cost the U.S. economy between $57 billion and $109 billion in 2016.[12]

The size of the premiums paid for cyber insurance also provides a sense of the size of the cybercrime market. A recent report stated that $4.85 billion in cyber risk premiums were paid in 2018 and projected that figure to reach $28.6 billion by 2026.[13] A recent report from the A.M. Best insurance credit rating agency found that "U.S. cyber insurance premiums grew again in 2019, up by 11%..." "Cyber insurance premiums will likely continue to rise . . . due to both rising claims costs and heightened risks... Over the past three years the number of cyber claims has doubled to 18,000 in 2019, from 9,000 in 2017."[14]

B. Parties Harmed by Cybercrime

Generally, we think of parties harmed by cybercrime falling into two groups. The first group are the parties whose system was breached, and the second are the other parties affected by the breach – the clients, customers, and vendors of the parties directly suffering the breach.[15] CAT LLC and the Plan Processor, FINRA CAT, clearly fall in the first group as they collect and store the information subject to cyber breach risk. It is their system that is subject to the cyber risk. Industry Members (and their investor clients) fall into the second group of affected parties as it is information about them and their activities that is supplied to the CAT.

---

10 Cybersecurity Ventures, "Global Cybercrime Damages Predicted to Reach $6 Trillion Annually By 2021," Copyright 2020, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ accessed August 2020.

11 Juniper Research, "Business Losses to Cybercrime Data Breaches to Exceed $5 Trillion By 2024," August 27, 2019, https://www.juniperresearch.com/press/press-releases/business-losses-cybercrime-data-breaches.

12 The Council of Economic Advisers, "The Cost of Malicious Cyber Activity to the U.S. Economy, February 2018, p. 1, https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

13 Allied Market Research website, *Cyber Insurance Market by Company Size and Industry Vertical: Global Opportunity Analysis and Industry Forecast, 2019-2026*, March 2020, https://www.alliedmarketresearch.com/cyber-insurance-market accessed August 2020.

14 Erin Ayers, "US cyber market keeps growing, but pace slowed: AM Best," Advisen Front Page News, July 22, 2020 accessed August 2020.

15 See, for example, Camico website, "Understanding First-Party and Third-Party Cyber Exposures," https://www.camico.com/blog/understanding-cyber-exposures accessed September 2020.

But that simple delineation does not cover all significant parties involved with supplying or accessing information from the CAT. The SROs also provide information to the CAT (some of the same information that is supplied by the Industry Members). As suppliers of information to the CAT, the interests of the SROs in cyber security at the CAT align with those of the Industry Members – a successful breach would compromise information on the CAT no matter if the original source were the Industry Members or the SROs. The SROs also, however, own and (through the CAT LLC Operating Committee) run the CAT. The SROs, therefore, face two risks arising from a cyber breach at the CAT: 1) directly from the breach of the CAT as owners of CAT LLC; and 2) indirectly from the exposure of information they supplied to the CAT (similar to the Industry Members).

The SEC is also a major user of the CAT in its efforts to regulate U.S. equity and option markets. The SEC's access to and use of CAT data is similar to that of the SROs and constitutes another source of cyber risk to CAT LLC. While the SEC does not own or directly operate the CAT, the CAT would not exist or operate absent the SEC's regulatory authority and associated oversight. The CAT, therefore, serves the regulatory needs of both the SROs and the SEC with the same functionality. In other words, the SEC's access to the CAT is every bit as broad as the SROs, who own and operate CAT LLC.

In the context of the CAT, therefore, a simple delineation of two types of affected parties is not adequate to describe and understand the parties potentially affected by a cyber breach at the CAT. In addition, there are some important atypical economic relations and regulatory considerations that affect the liability decisions associated with the CAT and its operations.

First, given that CAT and its activities are a regulatory mandate of the SEC, standard liability and indemnity approaches regarding the CAT's and the Plan Processor's scope and scale for decision-making cannot be straightforwardly applied. The CAT and the Plan Processor are substantially constrained in their cyber security program by mandates from the SEC that, in turn, involve significant input and advocacy on the part of other parties, including Industry Members.

Second, related parties include the Participants/SROs. While these parties are legally distinct from CAT and the Plan Processor, their involvement and economic linkage is substantial. For example, the Participants have ownership interests in CAT LLC and the Operating Committee of CAT LLC, on which the Participants are all members, chooses the Plan Processor. In addition, operational funding for the CAT (and therefore, the Plan Processor) comes entirely from Participants and Industry Members. Although there are regulatory users who access CAT, there are no "customers" for CAT's services in a conventional sense.

Third, CAT related decisions and actions of Industry Members are also mandated by the SEC and constrained by the SEC's oversight. There 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.

The typical economic distinctions between harms to parties with standard commercial relationships are much more amorphous with respect to the parties involved in the CAT. Any comprehensive analysis, therefore, requires careful distinctions and delineations between

standard commercial relationships and parties involved in the CAT to understand the CAT's economic considerations of cyber security.

C. Types of Bad Actors, Motivations, and Methods

Cybercrimes are conducted by both internal and external threat actors. According to a 2020 report by Verizon, approximately 70% of breaches in 2019 were caused by external actors with the other 30% being initiated by internal actors.[16] The motivations of these actors are often financial, but cyber breaches also happen for ideological or personal reasons. Nation-states, for example, have used cyber breaches to advance regime goals (often focusing on impeding the efforts of their geopolitical rivals) and obtaining information that might benefit them politically or economically.[17] Cybercriminals steal information to sell or extort payments from their targets. "Hacktivists" want to cause mayhem and influence the public. Sometimes, individuals are out for revenge against an entity or just want the bragging rights associated with a particularly brazen attack. At times, the malicious actors have multiple motivations – for example, ideology or revenge and financial remuneration. The 2020 Verizon report estimated that 90% of cyber breaches were motivated by financial considerations and 10% were initiated for espionage.[18] The bad actors were 55% organized crime, with the next highest type being nation-state or state-affiliated actors at around 10%. System administrators and end-users also comprised around 10% each of the bad actors.[19]

The methods used by the bad actors to perpetrate cyber breaches (alone or in combination) were around 45% hacking (use of stolen credentials), 22% error (e.g. mis-delivery), 22% social (e.g. phishing), 17% malware (e.g. password dumper), 8% misuse (privilege abuse), and 4% physical stealing (e.g. theft).[20]

D. Cyber Breaches Relevant to CAT, LLC Including Frequency, Severity, and Relative Difficulty of Implementation

There are several firms that provide summary level data on the types of cybercrime events, along with information on how frequently they occur and the associated severity of economic losses. One entity, Advisen, maintains a database of over 90,000 cyber events, and

---

16 Verizon, *2020 Data Breach Investigations Report*, p. 10, Figure 7.

17 See ScienceDirect website, "Hacktivists," https://www.sciencedirect.com/topics/computer-science/hacktivists accessed September 2020. Also see, Department of Homeland Security, "Commodification of Cyber Capabilities: A Grand Cyber Bazaar," 2019, p. 1 https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf accessed August 2020.

18 Verizon, *2020 Data Breach Investigations Report*, p. 10, Figure 8.

19 Verizon, *2020 Data Breach Investigations Report*, p. 11, Figure 10.

20 The total exceeds 100% because the bad actors could use one or more methods for each breach. See Verizon, *2020 Data Breach Investigations Report*, p. 7, Figure 2.

allows subscribers to perform customized searches.[21] In this paper, we have used the Advisen database to research frequency and severity for breaches we deemed specifically relevant to the types of data held on the CAT (Customer and Account Attributes and trade data).[22] We further refined the types of cyber events we believe could potentially affect the CAT by using Advisen data, other publicly available sources, and our own experience.

We have posited scenarios where malicious actors could make use of the CAT data should they successfully gain access to the data. These scenarios, while not exhaustive of every type of potential cyber breach, are the product of our understanding of the data available in the CAT and how it might be used to generate wrongful benefits for threat actors.[23] Some of the scenarios we discuss are more likely to be attempted, while others are more improbable. By their nature, the scenarios are general and therefore it is impossible to quantify the exact losses that could be generated by an unauthorized attack. As a frame of reference, based on the breach related losses experienced by Fortune 250 companies over the past decade, the losses range from the thousands of dollars to several billion.[24] Therefore, our approach for each scenario is to determine the relative ease of implementing the scenario, the relative frequency of how often it could be successfully carried out, and the conditional severity of the financial loss that could stem from the event (assuming the scenario was carried out successfully).

Relative Difficulty of Implementation: With respect to our assessment of the relative difficulty of implementation, we begin with an assumption that threat actors could breach the system, but then consider the number of databases the threat actors would need to breach, the extent to which the data would need to be manipulated for it to be useful, and the level of difficulty they would face in making use of that ill-gotten data to implement the strategy in the scenario.

Relative Frequency: The frequency assessment is based on our review of Advisen data for companies in the Fortune 250 for hacks similar to the ones we posit. We do not directly opine on the likelihood of successful hacks of the CAT, but instead use the Advisen data on successful hacks at large corporations to provide a subjective assessment of the relative frequency of a successful hack for each scenario we posit the CAT could face. We also consider the structural design of the CAT and the hurdles it presents to success of the strategy, as well as the

---

21 See Advisen website, https://www.advisenltd.com/data/cyber-loss-data/ accessed August 2020.

22 The PII that exists in the CAT is name, address, and birth year. This PII data will be in a "secure database physically separated from the transactional database…" See SEC, *March 17, 2020 Order*, pp. 12 and 20.

23 We believe that the scenarios we have posited are a useful way to characterize the economic risks facing the operation of the CAT, but we also recognize that any real-world hack could differ substantially from our scenarios in substantial ways.

24 The distribution of breach losses for the Fortune 250 extends from less than $1,000 to above $1 billion. The "Typical" breach loss is $471,000 while the "Extreme" breach loss is $93 million. See Cyentia Institute, *Information Risk Insights Study, A Clearer Vision for Assessing the Risk of Cyber Incidents*, p. 21, Figure 15.

attractiveness of the strategy because it could lead to a significant financial gain or achievement of a disruptive goal.

Conditional Severity: The severity of the financial loss (based on our review of Advisen data) that could stem from the event assuming the scenario was carried out successfully. We deem the loss severity for a particular type of breach to be *extreme* if we consider the exposure to be more than $100 million per event (95th percentile loss in the Advisen data), *high* if we consider the exposure to be approximately $5-50 million, *medium* if we consider the exposure to be approximately $500,000, and *low* if we consider the exposure to be approximately $50,000 or less.[25]

Below we first discuss summary descriptive statistics regarding cyber breaches and then the types of breaches we believe are specific risks faced by the CAT.

1. Summary Level Data

Our review of available information on various aspects of cyber breaches led us to focus on periodic reports prepared by Ponemon Institute/IBM Security, Verizon, and Cyentia. While these entities do not report the same information in the same way, there appears to be a consensus that malicious attacks are the primary reasons for cyber breaches, and that the risk of a breach increases with firm size. The Fortune 250 are particularly frequent targets.[26] Furthermore, the costs[27] associated with dealing with large, mega, and extreme[28] breaches, as

---

25 These amounts are based on the distribution of breach losses for the Fortune 250 over the past 10 years. See Cyentia Institute, *Information Risk Insights Study, A Clearer Vision for Assessing the Risk of Cyber Incidents*, 2020, p. 21, Figure 15.

26 The top 250 firms of the Fortune 1000 are nearly five times more likely to have a breach than the bottom 250. See Cyentia Institute, *Information Risk Insights Study, A Clearer Vision for Assessing the Risk of Cyber Incidents*, 2020, p. 8.

27 The costs in the IBM Security report include both the direct and indirect expenses incurred by the organization. Direct expenses include engaging forensic experts, legal fees, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and services. Indirect costs include in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished customer acquisition rates. See Ponemon Institute and IBM Security, *Cost of a Data Breach Report 2020*, p. 72. The costs in the Cyentia/Advisen report include losses related to productivity, response, replacement, competitive advantage, fines and judgments (including legal fees), and reputation. See Cyentia Institute *Information Risk Insights Study, A Clearer Vision for Assessing the Risk of Cyber Incidents*, 2020, p. 16. Also see, Teresa Suarez, "A Crash Course on Capturing Loss Magnitude with the FAIR model," *Fair Institute* Website, October 20, 2017, https://www.fairinstitute.org/blog/a-crash-course-on-capturing-loss-magnitude-with-the-fair-model accessed August 2020.

28 The IBM Security report notes several levels of a mega breach, the first is 1 million to 10 million records and the largest is 50 million or more records. We refer to the first as a large breach (1 million to 10 million records) and the other as a mega breach (more than

shown in the table below, run from $10 million to $100 million or more. The costs of a breach include such items as detection and escalation costs, notification costs, post-data-breach response costs, and lost business costs.[29]

Figure 1[30]

Summary of Cyber Breach Report Data

			Reason for Breaches			Cost of a Breach		
Reporting Entity	Report year	Sample	Malicious Attacks	Insider Errors	Observed Breach Frequency	Large Breach > 1 million records	Mega Breach > 50 million records	Extreme Event 95th percentile cost
IBM Security	2020	Study of 524 organizations	52%	48%	N/A	$50 million for a breach of more than 1 million records	$392 million for a breach of more than 50 million records	N/A
Verizon	2020	Study of 157,525 incidents, 32,002 met quality standards and 3,950 were confirmed data breaches	78%	22%	N/A	N/A	N/A	N/A
Cyentia/Advisen	2020	Study of 56,000 cyber events experienced by 35,000 organizations over the last decade	N/A	N/A	114 of the Fortune 250 experienced a breach in a twelve-month period	N/A	Better than 50% chance of at least $10 million with the exposure of 100 million records	The cost of extreme events (95th percentile) in the Fortune 250 approaches $100 million or more

2. Breach Data Specifically Relevant to CAT, LLC

The CAT data is unique and valuable because it is the only data repository that collects and holds Customer and Account Attribute data and all trading data from all the U.S. equity and option exchanges.[31] The compromise of this data, as discussed in further detail below, could

50 million records). See Ponemon Institute and IBM Security, *Cost of a Data Breach Report 2020*, pp. 10 and 67. The Cyentia/Advisen report does not use the term "mega breach" but does note the cost of a breach of 100 million records. We label this as a "mega breach" to compare to the data in the IBM Security report. In addition, the Cyentia/Advisen also provides an "extreme event" figure on a cost basis alone, no records mentioned. Thus, we provided this information in its own column. See *Cyentia Institute Information Risk Insights Study, A Clearer Vision for Assessing the Risk of Cyber Incidents*, 2020, p. 3.

29 See Ponemon Institute and IBM Security, *Cost of a Data Breach Report 2020*, p. 7.

30 See Ponemon Institute and IBM Security, *Cost of a Data Breach Report 2020*, pp. 3, 30, 66-67, Verizon *2020 Data Breach Investigations Report*, pp. 6-7, Figure 2, and Cyentia Institute *Information Risk Insights Study, A Clearer Vision for Assessing the Risk of Cyber Incidents*, 2020, pp. 3, 4, and 8.

31 See SEC website, "Rule 613 (Consolidated Audit Trail)," https://www.sec.gov/divisions/marketreg/rule613-info.htm.

cause harm in the form of investor losses, reputational harm, interference with market surveillance by the SROs and the SEC, and loss of investor confidence in the markets themselves. For the exchanges, the scale of potential liability could significantly financially harm those entities that constitute the national market system in the U.S. securities markets.[32]

More specifically, the CAT Customer and Account Attributes database (the CAIS database) is the only database that exists that aggregates, across all U.S. stock exchanges, elements of PII (name, address, birth year)[33] for the over 100 million people, companies, and trusts,[34] that hold accounts trading U.S. equities and options. The CAT trade database (the MDS database)[35] is the only database that aggregates, across all U.S. exchanges, all of the exchange-based equity and option trades by customer ID for those persons and entities. Further, the data in the CAT CAIS database is stored and processed in a separate, independent system from the MDS database. These systems are operated by different personnel. The data in the CAIS and MDS databases are encrypted independently of each other using different keys. The trade data (MDS database) is anonymized; there is no PII data present. Customer and Account Attributes data (CAIS database) is only accessible with limited permission and no data extraction is allowed,

---

32 The Securities Exchange Act of 1934 (Exchange Act) codified the legal status of exchanges as self-regulatory entities (SROs) under federal law. The Exchange Act vested exchanges with the responsibility to oversee trading on their respective markets and to regulate conduct of their members, including the responsibility to enforce compliance by their members with the Exchange Act. Thus, the Exchange Act reflected Congress' determination to rely upon self-regulation as a fundamental component of the oversight and supervision of U.S. securities markets and their members. See Memorandum from SEC Division of Trading and Markets to SEC Market Structure Advisory Committee dated October 20, 2015 with the subject "Current Regulatory Model for Trading Venues and for Market Data Dissemination," pp. 1-2, https://www.sec.gov/spotlight/emsac/memo-regulatory-model-for-trading-venues.pdf.

33 The PII that exists in the CAT is name, address, and birth year. This PII data will be in a "secure database physically separated from the transactional database…" See SEC, *March 17, 2020 Order*, pp. 12 and 20.

34 There are approximately 330 million people in the United States. See United States Census Bureau website, the U.S. and World Population Clock, https://www.census.gov/popclock/ accessed September 2020. According to a FINRA study, around 32% of the national population have investments in non-retirement accounts (330 million times 32% = 105.6 million non-retirement accounts. See FINRA Investor Education Foundation, "Investors in the United States, A Report of the National Financial Capability Study," FINRA Investor Education Foundation, December, 2019, p. 3.

35 See SEC, *March 17, 2020 Order*, p. 12. SEC., *Order Approving CAT, The Limited Liability Company Agreement of CAT LLC*, Appendix C-4 and Appendix D-14.

only interactive queries. Queries of any CAT data can only be done by the SEC and SROs via private line access; no public internet access.[36]

[36] All CAT Data must be encrypted at rest and in flight using industry standard best practices. See SEC, *Order Approving CAT, The Limited Liability Company Agreement of CAT LLC*, p. 62, Appendix D-11, and D-14.

Figure 2[37]

Overview of the CAT Databases and How They Can be Accessed

Type of Data	PII Related		Trade Related
System / Database	CAT Customer ID (CCID) Subsystem	Customer and Account Information System (CAIS)	Market Data System (MDS)
Purpose	Receives Transformed Identifiers (TIDs) from Industry Members and generates a corresponding CAT Customer ID (CCID) for each TID. A received TID may be a transformed value of an ITIN, SSN, or EIN associated with an account holder or authorized trader. The generated CCID is a globally unique value that is unknown to and not shared with the original Reporter of the customer information.	Collects the Customer and Account Attributes and other identifiers (e.g. Prime Broker ID and Clearing Broker) from the Industry Members and links this data with the corresponding unique CCID provided by the CCID Subsystem.	Collects all order event information for National Market System securities and OTC equity securities, across all markets, from the time of order inception through routing, cancellation, modification, execution, and allocation. The Participants and Industry Members (i.e. brokers) handling the orders are also collected.
Data Contained	TID collected from the Industry Member and the corresponding CCID generated for each TID.	CCID Customer Attributes include name, address, year of birth, and the individual's role in the account. For legal entities, it includes name, address, employee identification number, and legal entity identifier. Account Attributes include account type, customer type, date account opened, and large trader identifier.	All Market Data, including the Firm Designated Identifier (FDID) for the Industry Member account associated with each event. CCIDs associated with each FDID (mapping provided to the MDS by CAIS) are also available.
Access	Regulators (SEC and SROs) have limited and monitored ability to submit a TID of interest and obtain the corresponding CCID. All CAT query interfaces are designed to be accessed only via private lines established with the SROs and the SEC; query via the internet is not supported.	Access to data is tiered and authorized based on role. Only a limited number of appropriately authorized users determined to have a need to know by their regulatory organization are entitled to the most sensitive information (e.g. name, address, birth year). Access is guided by "need to know" and "least privilege" principles. All CAT query interfaces are designed to be accessed only via private lines established with the SROs and the SEC; query via the internet is not supported.	Authorized users of the SROs and the SEC have access to all trade data via an online targeted query tool, a user-defined direct query tool, and bulk extracts. Extraction of CAT Data is based on permissions granted by the Plan Processor. All CAT query interfaces are designed to be accessed only via private lines established with the SROs and the SEC; query via the internet is not supported.

[37] Please note this is based on the CAT NMS Plan and amendments. See, SEC, *Order Approving CAT*, pp. 47-48, SEC, *Order Approving CAT*, *The Limited Liability Company Agreement of CAT LLC*, p. 62, Appendix C-7 to C-9, Appendix D-14, and D-33 to D-34, SEC, *March 17, 2020 Order*, pp. 2, 4-5, 12, 15 and 20 and *CAT Reporting Technical Specifications for Industry Members*, Version 3.1.0 r2, April 21, 2020, p. 1 and 5-6.

Given the unique nature of the CAT data set, we are unable to find cyber breach events that exactly mirror potential CAT data breaches. However, we believe review of cyber breach events related to Finance and Insurance companies with greater than $1 billion revenue can serve as a helpful proxy. We used the Advisen database and other public sources to search for information on cyber breach events related to such companies.

The summary chart below displays the results of filtering the Advisen database to obtain cyber breach data over the past 10 years associated with companies with $1 billion revenue or greater that are classified as Finance and Insurance companies in the North American Industry Classification system.[38]

[38] We deemed application of these filters to be reasonable since the CAT will hold more records than most large (>$1 Billion) corporations, and because the data the CAT stores is from companies that fall into the Finance and Insurance classification.

Figure 3[39]

Advisen Cyber Breach Data: Finance and Insurance Companies with $1 Billion Plus in Revenue

NAICS 52 Finance and Insurance + Equifax -- Revenue $1B or Greater -- Last 10 Years				
	Frequency		Severity	
	(# of Incidents per Company)		($M Lost Per Company)	
Incidents/Assets Compromised	**Average**	**Median**	**Average**	**Median**
All Cyber Incidents				
Total	13.3	3	24.5	3.6
Type of Cyber Incident				
Data Privacy	13.4	3	23.1	3.6
Data - Malicious Breach	8.8	2	23.0	3.2
Data - Physically Lost or Stolen	4.1	2	4.1	1.7
Data - Unintentional Disclosure	7.5	2	6.0	2.7
Identity - Fraudulent Use/Account Access	3.4	2	1.1	0.6
Phishing, Spoofing, Social Engineering	1.6	1	1.6	0.9
Privacy - Unauthorized Data Collection	1.8	1	15.6	2.0
Skimming, Physical Tampering	3.7	1	2.8	0.9
Network Security	1.6	1	4.1	3.1
Network/Website Disruption	1.6	1	4.3	3.3
Cyber Extortion	No data	No data	No data	No data
Industrial Controls & Operations	1.0	1	2.8	2.8
Tech E&O	2.0	1	13.0	2.0
Network/Website Disruption	1.5	1	21.8	3.8
Cyber Extortion	1.8	1	4.1	1.9
	Frequency		**Severity**	
	(# of Incidents per Company)		**($M Lost Per Top 10 Companies)**	
Type of Asset Compromised	**Average**	**Median**	**Lowest**	**Highest**
Personal Information	13.7	3		
Personal Identifiable Information (PII)	3.4	1	9.1	21.6
Personal Financial Information (PFI)	13.2	3	11.7	2470.1
Personal Health Information (PHI)	4.4	2		
			($M Lost Per Top 2 Companies)	
Corporate Losses	1.8	1	**Lowest**	**Highest**
Corporate Loss of Digital Assets	1.2	1	8.8	22.9
Corporate Loss of Business Income/Services	1.8	1	373.5	472.0
Corporate Loss of Financial Assets	1.0	1		

Malicious breaches are the most common and the most expensive.[40] Correspondingly, the Advisen data shows that for Finance and Insurance companies with $1 billion or greater in revenue that had a malicious cyber breach, those firms had 8.8 malicious cyber breaches, on

39 Data pulled from Advisen Cyber OverVue, https://insite20twenty.advisen.com, on September 11, 2020.

40 See Ponemon Institute and IBM Security, *Cost of a Data Breach Report 2020*, pp. 29 and 31.

average (median of 2), over the past 10 years.[41] The average cost of these malicious breaches was $23.0 million with a median of $3.2 million.[42]

The asset most frequently compromised was personal financial information ("PFI").[43] We examined the top 10 PFI loss breaches from the Advisen database and found that the top 10 losses ranged from $11.7 million to $2.5 billion (Equifax).[44] The second highest loss for PFI after Equifax was $188.7 million (Wells Fargo).[45]

The data in the table above also includes frequency and losses from internal cyber related errors. These events typically include things like software errors or a when a human mistake involving a computer is made. For example, the top ten largest error-related cyber loss events

---

41 The large difference between the median of 3 and average of 13.3 breaches for this data set is attributable to the large degree of variance in the number of breaches by firm. In other words, a few firms experienced a very large number of breaches, increasing the average relative to the median.

42 The large difference between the median cost of $3.2 million and average cost of $23.0 million for a malicious breach in this data set is attributable to the large degree of variance in the cost per breach by firm. In other words, a few firms experienced a very large cost per breach, increasing the average relative to the median.

43 Advisen defines PFI or personal financial information as credit/debit card details, social security numbers, banking financial records (account numbers, routing numbers, etc.). Advisen defines PII or personal identifiable information as data containing identifying information, including name, address, e-mail, date of birth, gender, etc. See Advisen's Cyber OverVue User Guide, January 2020, p. 26. Also, "The compromise of the Confidentiality of Personal data leads the pack among attributes affected in breaches," See Verizon *2020 Data Breach Investigations Report*, p. 29. "More than half of all cybercrime incidents investigated by CyberScout involved financial fraud, one of the most common forms of identity theft." See Advisen, *Quarterly Cyber Risk Trends: Global Fraud is Still on the Rise*, sponsored by CyberScout, Q2 2019, p. 2.

44 See the PFI Top 10 cyber loss events as of September 11, 2019 as obtained from Advisen Cyber OverVue, insite20twenty.advisen.com. Equifax is coded under NAICS 56 Administrative and Support and Waste and Management Remediation Services in Advisen's Cyber OverVue, but it is coded as NAICS 522320 – Financial Transactions Processing, Reserve, and Clearinghouse Activities in Advisen's MSCAd database (see Advisen website, www.advisenltd.com). In speaking to Advisen's product manager, he stated that in Cyber OverVue, the NAICS code is taken directly from Advisen's company information provider, in this case S&P. In MSCAd, which is Advisen's legacy system that they are moving away from, the NAICS code is a translation of the SIC code. These differences in industry classification between the two systems can sometimes create misalignments, but rarely. CRA manually added Equifax to the NAICS 52 Finance and Insurance peer group based on its potential applicability in size and type of assets (PII or PFI) compromised.

45 See the PFI Top 10 cyber loss events as of September 11, 2019 as obtained from Advisen Cyber OverVue, insite20twenty.advisen.com.

from the events underlying the table above (in the corporate losses section) ranged from $472.0 million down to $7.3 million. The top two were $472.0 million for Knight Capital Group and $373.5 million for TSB Bank. Both were caused by IT errors. For Knight Capital Group, a glitch in new trading software caused Knight Capital Group's order router to send more than four million orders into the market when it was supposed to fill in just 212 customer orders.[46] For TSB Bank, customers lost access to their accounts or saw information of accounts owned by others after TSB Bank transferred the records and accounts of its 5.2 million customers from one system to another. All of the top ten error-related cyber loss events impacted a company's ability to conduct business and generate revenues.[47] While the CAT does not support a specific company's ability to conduct business and generate revenues it does affect the ability of the SEC and the SROs to oversee and regulate market activities. However, it is our understanding that if the CAT has appropriate backups that have not been maliciously encrypted, this type of attack can be recovered from.[48] While regulatory oversight could be delayed by the error, the oversight activities can be resumed after a relatively brief period devoted to bringing up the backup systems. Overall, we note that internal cyber related errors can lead to very large losses that represent additional liability exposure to the CAT.

To further refine the types of cyber breaches we believe could potentially affect the CAT, we searched public sources and relied upon our experience to posit scenarios we believe reflect how data from possible cyber breach attacks/events could be misused.

We believe threat actors could seek to breach the CAT to attempt the following:

(1) Hold Data Hostage

(2) Identity Theft

(3) Algorithm Reverse Engineering

(4) Fake Data Insertion to Wrongfully Incriminate

(5) Data Removal or Insertion to Hide Fraud

(6) Trading on Non-Public Information

(7) Competitive Intelligence – Customer Lists

(8) Discovery of Regulatory Investigation that Could be Used to Harm Someone's Reputation

We address the scenarios below and describe our estimation of the ease of implementation, frequency and severity risk of each.

(1) Hold Data Hostage

---

46 See Corporate Business Income/Services Top 10 cyber event losses as of September 11, 2019 as obtained from Advisen Cyber OverVue, insite20twenty.advisen.com.

47 See Corporate Business Income/Services Top 10 cyber event losses as of September 11, 2020 as obtained from Advisen Cyber OverVue, insite20twenty.advisen.com.

48 Interview with William Hardin, VP, Charles River Associates, August 11, 2020.

A bad actor could seek to ransom CAT data in several ways. Many of them are derivative of the other scenarios we posit later in this report.

(a) Threaten to publicly release confidential Customer and Account Attribute data or trade data to harm a firm's or investor's reputation

(b) Threaten to keep data encrypted (denial of service) to prevent its use by regulators

(c) Threaten to sell trading data regarding an account that could allow reverse engineering a trading algorithm

(d) Threaten to make short position data public

Each of these is discussed in further detail:

(a) Threaten to publicly release confidential Customer and Account Attribute data or trade data to harm a firm's or investor's reputation

Under this scenario, if a bad actor obtained either Customer and Account Attribute data or trade data from the CAT it would be difficult for the bad actor to monetize the information without the ability to associate the trade data with the Customer and Account Attribute data to identify the parties involved in the trade as bad actors historically have done.

To limit the potential value of the information, the SEC mandated that the CAT limit the identifying information it stores. Information such as a social security number, brokerage account number, and other high value PFI items are not stored by the CAT. The CAT stores only less sensitive PII information including name, address, and birth year within the CAT Customer and Account Attributes database (CAIS).[49] Also, the trade data stored by the CAT does not disclose the name of the person or company behind the trade. Rather, the account owner behind the trade is identified by a CAT Customer ID (CCID) that is a globally unique CCID for each account owner that is unknown to and not shared with the original CAT Reporter Industry Member. This CCID is held within the CAT's CCID and CAIS databases.[50] To determine the account owner, one would need access to the system that links the CCID to the Customer and Account Attributes data, the CAT Customer and Account Information System (CAIS). The trade data and the CAIS data are stored on separate encrypted systems. Thus, a bad actor would need access to the trade data and the CAIS data for each individual/company in order to find out which trades related to which individuals/companies and which brokers were used by these individuals/companies. Therefore, we see limited possibility or value in a hacker seeking to threaten a brokerage firm or other investor with the release of Customer and Account Attributes.

With respect to an attempt to hold hacked CAT trade data hostage, we note that all the trade data is encrypted with the client anonymized, making it unlikely that a hacker could successfully identify who to threaten. The bad actor would need to have the CAIS data and trade

---

49 See SEC, *March 17, 2020 Order*, pp. 4-5 and SEC, *Order Approving CAT, The Limited Liability Company Agreement of CAT LLC*, p. 4, Appendix C-7 to C-9, Appendix D-14, and D-33 to D-34,

50 See SEC, *March 17, 2020 Order*, pp. 2, 4-5.

data to determine which clients and client trades were associated with a broker or investor. Given that the CAT keeps encrypted CAIS data and encrypted trade data in separate databases, a data incident to obtain and exploit both sets of data would be difficult. We recognize that crime syndicates are publishing information to their blogs,[51] and if they released even partial information to the public, this could damage the reputation of the CAT. The breach would show weaknesses in the security of the CAT and translate into potential reputational harm to not only the CAT, but also possibly the SEC and the SROs. Overall, we believe this scenario would be of average difficulty to implement, will occur infrequently (if at all), but have low to medium loss severity if successful.

(b) Threaten to keep data encrypted (denial of service) to prevent its use by regulators

If a hacker were able to disrupt the CAT and impose another level of unauthorized and malicious data encryption in an attempt to ransom its decryption, this could affect the SEC's ability to conduct investigations as well as the SROs' ability to meet their oversight obligations.[52] A particular concern for a system held by ransomware is the inability of the affected firms to access their information and maintain operations for their customers. However, it is our understanding that if the CAT has appropriate backups that have not been maliciously encrypted, this type of attack can be recovered from.[53] While regulatory oversight could be delayed by a ransomware attack, the oversight activities can be resumed after a relatively brief period devoted to bringing up the backup systems. We deem a successful ransomware scenario to be highly unlikely, assuming adequate backup systems and protocols, as a hacker is likely to perceive that collecting a ransom from the regulators has a very low probability. We believe this scenario would be of average difficulty to implement, will occur infrequently, and have low to medium severity if successful.

(c) Threaten to sell trading data regarding an account that could allow reverse engineering a trading algorithm

This scenario would be difficult to implement given the bad actor would need to access the trade data as well as the CAIS (assuming the bad actor could not otherwise determine the

---

51 Per William Hardin, VP Cybersecurity and Incident Response Services, Charles River Associates, Inc.

52 Under the Exchange Act, a variety of SROs, including national securities exchanges and FINRA, exercise extensive oversight over securities broker-dealers, stock exchange members and listed companies, and other market intermediaries. Stock exchanges were the original SROs that governed the trading of securities and regulated their members well before the creation of the Securities and Exchange Commission and the current statutory framework formalizing their SRO status. See Commissioner Luis A. Aguilar, U.S. Securities and Exchange Commission, "The Need for Robust SEC Oversight of SROs," May 8, 2013, footnote 2, https://www.sec.gov/news/public-statement/2013-spch050813laahtm accessed August 2020.

53 Per William Hardin, VP Cybersecurity and Incident Response Services, Charles River Associates, Inc.

who the trade data was associated with[54]). Gaining access to multiple encrypted CAT databases to retrieve multiple categories of data, stored in separately secured areas would be difficult. It would also be difficult for the bad actor to figure out who the trade CCID account owner was without access to the CAIS. Overall, the bad actor would need to access the trade data, analyze the data for algorithmic trading, and determine who the CCID account owner is in order make the threat real. Next, they would have to credibly threaten that firm that their trades would be released or sold to someone that could reverse engineer their algorithms, which is a complex and difficult task. We think that, at worst, the threatened firm might pay a moderate ransom to prevent its trades from being in unknown hands. Thus, we believe this scenario would be very difficult to implement, will occur infrequently, and have high to extreme severity if successful.

(d) Threaten to make short position data public

If a bad actor were able to use the CAT trading and CAIS data to successfully determine that an investor holds a significant short position in a particular stock, in theory, that hacker could try to threaten that investor that their position information would be made public. We deem this scenario as improbable and unlikely. First, as discussed above, determining both the investor identity and the position held by that investor would be difficult. Second, there is a significant risk to the hacker that the investor would not care that their short position was made public. Thus, we believe this scenario would be of average difficulty to implement, will occur infrequently, and have medium severity if successful.

(2) Identity Theft

We believe that one of the most likely goals of wrong-doers seeking to hack the CAT would be to attempt to steal Customer and Account Attribute data (within the CAIS database) for the millions of account holders in the system. We note that significant effort has been made in designing the CAT to reduce this risk. This includes encrypting of the Customer and Account Attribute data and limiting the underlying PII to less sensitive information: name, address and birth year (no PFI data - no social security numbers, no account numbers, and no dates of birth). Importantly, there are strict limitations on access to the CAIS database. Access to the CAIS is on a "need to know" and "least privileged" basis and cannot be obtained from public internet connectivity.[55]

An example of how a hacker could take advantage of less sensitive PII data (name, contact information, and a reservation) can be seen in the recent breach at the Ritz Carlton's London hotel. In August of 2020, the hotel suffered a cyber breach of its food and beverage system. The bad actor used the customer information in this system to pose as a Ritz employee to confirm the reservation and payment card details with individuals with the upcoming reservations. The card details received based on these calls were used to spend thousands of pounds of victims' money.[56] If a hacker were able to get CAT Customer and Account Attribute

---

54 We can envision that a bad actor might be able to deduce who the trade data was associated with based on certain characteristics of quantity, size, or through other means.

55 See SEC, *March 17, 2020 Order*, pp. 12 and 20 and SEC, *Order Approving CAT, The Limited Liability Company Agreement of CAT LLC*, Appendix D-14.

56 See Julian Hayes, "Double extortion: An emerging trend in ransomware attacks," *Advisen Front Page* News, August 21, 2020,

data and determine the brokerage firm at which a particular investor held their account, the hacker could call that investor posing as an employee of the broker and seek to "confirm account information." This could lead to substantial investor losses. This scheme could then be repeated on large numbers of investors.

Had the CAT Customer and Account Attribute data included social security numbers and birth dates, this information could be even more easily monetized by either identity/credit theft or selling the data in bulk on the dark web. William Hardin, VP and leader of Charles River Associates Cybersecurity Incident Response Practice stated, "the most readily available easily monetized form of hacked data on the dark web is PII."[57]

Verizon reported that the compromise of personal data occurs in 77% of the Finance and Insurance industry cyber breaches and that cyber-attacks are mostly carried out by external actors who are financially motivated to get easily monetized data.[58] According to the data in the Advisen database, personal information is the most common type of data compromised in a cyber breach. The Advisen database shows that Finance and Insurance companies with $1 billion or greater in revenue that had a PII breach had an average of 3.4 breaches (a median of 1) over the past 10 years.[59] The frequency and severity of PII breaches is much lower than PFI breaches. Thus, based upon this history, we believe the CAT substantially reduced its relative exposure to the frequency and severity of breaches related to personal information by not including PFI data in the CAT. While this design feature is appropriate, CAT remains a tempting target for cybercriminals as it will have one of the largest accumulations of personal data ever assembled. The possibility of an extreme event should not be ignored.

We reviewed the top 10 PII cyber breaches underlying these figures and summarized them in the table below. We found the lowest loss was $9.1 million while the highest was $21.6 million. While an imperfect measure, generally the more records exposed,[60] the higher the loss amount. We note that Equifax is not included in the PII breach data because that breach included access to PFI (social security numbers). The Equifax loss was $2.5 billion and is the largest publicly disclosed PFI breach. It has been reported that this loss resulted from Equifax leaving

---

https://www.advisen.com/tools/fpnproc/fpns/articles_new_35/P/375350842.html?rid=375350842&list_id=35 accessed August 2020.

57 Interview with William Hardin, VP, Charles River Associates, August 11, 2020.

58 Verizon, *2020 Data Breach Investigations Report*, p. 52.

59 See Advisen Cyber OverVue, insite20twenty.advisen.com.

60 The firms working in the cyber risk industry typically use the number of records exposed/stolen as a metric to describe the relative size and seriousness of a breach. While there is some correlation between the number of records exposed and the ultimate cost of the breach, this metric is imperfect as it does not consider the relative value of the records exposed or how they might be used. However, as long as one recognizes those limitations, we believe the number of records exposed can be a useful descriptor. We note that the CAT will contain massive amounts of data, including information on hundreds of millions of accounts, making it much bigger than some companies we review for comparison.

itself significantly exposed to hacking because it failed to implement various software security patches in a timely manner. In relation to the Equifax breach, the number of records potentially exposed at the CAT could be even larger. But since the CAT will only include less sensitive PII (name, address, birth year) and not PFI (social security number, account numbers), we believe the Equifax loss of $2.5 billion can be seen as an upward bound of the exposure a Customer and Account Attribute data breach at the CAT could generate.

Based on the descriptions provided by Advisen, the most similar PII breach to what CAT might experience in the list below is the E*TRADE hack, where a bad actor accessed their customer database and exported stolen customer data including names, residential addresses, phone numbers, and email addresses. These addresses were allegedly taken so the bad actors could start their own securities brokerage. Overall, the hackers compromised customer databases containing the personal information of more than 5 million customers, leading to a $12.9 million loss.[61] While there will be fewer elements of PII stored at the CAT (name, address, and birth year) than at E*TRADE (name, address, phone number, and email address), we again note there will be orders of magnitude more individuals' records at the CAT.

Figure 4[62]

Advisen Top 10 PII Cyber Breaches for Finance and Insurance Companies with $1 Billion Plus in Revenue

	PII Top 10					
	* represents simulated values					
	Company Name	Type of Incident	Incident Date	Records Exposed	Loss Amount	Asset Compromised
1	Industrial & Commercial Bank of China Ltd	Data - Malicious Breach	1/1/2017	117	$21,602,135*	PII
2	Morgan Stanley	Data - Malicious Breach	3/1/2016	14,256,250	$18,571,612*	PII
3	Swedbank AB	Data - Malicious Breach	1/1/2016	178	$16,910,448*	PII
4	E*TRADE Financial Corporation	Data - Malicious Breach	11/1/2013	5,000,000	$12,856,871*	PII
5	Wells Fargo & Co	Data - Malicious Breach	7/1/2016	5	$11,187,547*	PII
6	Wells Fargo & Co	Data - Malicious Breach	5/22/2017	5	$10,225,135*	PII
7	Aetna Inc	Data - Malicious Breach	11/22/2016	5	$10,001,613*	PII
8	Wells Fargo & Co	Data - Malicious Breach	3/16/2016	4	$9,300,114*	PII
9	State Farm Mutual Automobile Insurance Company	Data - Malicious Breach	2/27/2017	2	$9,241,348*	PII
10	Wells Fargo & Co	Data - Malicious Breach	9/11/2015	26	$9,128,562*	PII

As noted above, the Advisen database showed that for Finance and Insurance companies with $1B in revenue or more that had a PII breach, these breaches occurred with a frequency of

---

61 See the PII Top 10 cyber loss events as of September 11, 2019 as obtained from Advisen Cyber OverVue, insite20twenty.advisen.com.

62 "Advisen has developed a proprietary loss amount model to help users make more informed decisions on cyber risk by enhancing how it is being quantified. The resulting analytics, when viewed in tandem with our benchmarking analyses, will provide a comprehensive picture of an organization's potential cyber loss exposure, as well as better guidance on the type and amount of cyber insurance to purchase. The model looks at a combination of more than 70 different variables across more than 100,000 cyber events in Advisen's proprietary cyber loss data to calculate simulated financial loss

3.4 times on average over a 10-year period (median of 1). The range for the top 10 PII breaches was $21.6 million to $9.1 million.

The second highest PFI breach, after Equifax, is the $188.7 million loss suffered by Wells Fargo & Co. (Wells Fargo), which resulted from the bank allowing its employees to access customers' personal information, and in some cases forging data, to subscribe them to products, such as credit cards. Lawyers representing aggrieved customers have said the bank may have opened about 3.5 million unauthorized accounts.[63]

If the CAT stored social security numbers and account numbers (as was originally planned before the amendments), the exposure on a successful hack would be extreme. But, because the CAT Customer and Account Attribute data is limited to name, address and birth year, we believe that risk is mitigated to some degree. In summary, we suggest CAT Customer and Account Attribute data will be of medium interest to hackers and conclude this scenario would be relatively less difficult to implement, will occur with moderate frequency, and likely have medium to high severity if successful. An extreme event cannot be ruled out primarily because of the quantity of Customer and Account Attribute data being held at the CAT.

(3) Algorithm Reverse Engineering

Algorithmic trading uses a computer program that follows a defined set of instructions (an algorithm) to execute a trade. The trades can be executed at a speed and frequency that is impossible for a human trader. The algorithmic trading market size was $11.1 billion in 2019 and expected to grow to $18.8 billion by 2024.[64,65] Algorithmic trading is responsible for approximately 60-73% of all U.S. equity trading.[66] The two largest firms, Virtu Financial, Inc.

---

amounts by incorporating quantile regression analyses that look at data relationships across different quantiles to establish a range of potential impacts. The model is recalibrated on an ongoing basis to account for changes in data relationships as Advisen's cyber loss database continues to grow." See Advisen's Cyber OverVue User Guide, January 2020, p. 22. See also the PII Top 10 cyber loss events as of September 11, 2019 as obtained from Advisen Cyber OverVue, insite20twenty.advisen.com.

63 See the PFI Top 10 cyber loss events as of September 11, 2019 as obtained from Advisen Cyber OverVue, insite20twenty.advisen.com.

64 Research and Markets, *Algorithmic Trading Market by Trading Type, Component, Deployment Mode, Enterprise Size, and Region – Global Forecast to 2024*, https://www.researchandmarkets.com/reports/4770543/algorithmic-trading-market-by-trading-type#rela0-4833448 accessed November 2020.

65 We note that high frequency trading (HFT), a major subset of algorithmic trading, has experienced higher costs and lower profitability in the past few years. See Gregory Meyer, Nicole Bullock and Joe Rennison, "How high-frequency trading hit a speed bump," *Financial Times*, January 1, 2018, https://www.ft.com/content/d81f96ea-d43c-11e7-a303-9060cb1e5f44 accessed August 2020.

66 Research and Markets, *Algorithmic Trading market – Growth, Trends, and Forecast (2020-2025)*, https://www.researchandmarkets.com/reports/4833448/algorithmic-trading-market-growth-trends-and#rela4-5125563 accessed August 2020.

("Virtu") and Citadel "account for around 40 percent of daily U.S. trading flow."[67] Virtu is the largest public algorithmic trading firm, with a market cap of $4.56 billion.[68,69] Furthermore, Citadel, the nation's biggest equity and options market maker, is responsible for one in every five stock trades in America and 40% of the retail volume.[70]

Algorithmic trading plays an important role in making the U.S. markets more efficient. Academic research has shown that algorithmic trading significantly reduces bid-ask spreads and speeds price discovery.[71]

Assuming the trading data of the CAT LLC was breached and decrypted, we assess that, while difficult, that data could be used to reverse engineer the proprietary trading algorithms of algorithmic trading firms. The loss to a firm whose algorithm was compromised in this way would be the cost of developing the algorithm plus any forgone profits that could have been expected to accrue to the firm over a reasonable period of time.

For example, as of January 2020, Citadel is suing a rival for allegedly taking details of a key Citadel trading strategy which Citadel has stated cost more than $100 million to develop and which generates many millions of dollars each year.[72]

Although we assess that using the CAT data to reverse engineer a trading algorithm would take significant expertise and time, the trading strategies that use these algorithms are highly valuable. In addition, the concentration of profitability among a small number of players

---

67 AllAboutAlpha, "High-Frequency-Trading Firms: Fast, Faster, Fastest," April 2, 2019, https://www.allaboutalpha.com/blog/2019/04/02/high-frequency-trading-firms-fast-faster-fastest/ accessed November 2020.

68 See Capital IQ website, https://www.capitaliq.com/CIQDotNet/Financial/Capitalization.aspx?CompanyId=133624510 accessed November 6, 2020.

69 Interestingly, Virtu was the victim of a recent social engineering hack. A hacker seized control of the email account of one of its executives. The email account was used to send two fraudulent wire transfers totaling $10.8 million to bank accounts in China. See Alexander Osipovich, "High Speed Trader Virtu Discloses $6.9 Million Hacking Loss," *Dow Jones News Service,* August 11, 2020 accessed December 2020.

70 Nathan Vardi, "Finance Billionaire Ken Griffin's Citadel Securities Trading Firm Is On A Silicon Valley Hiring Binge," June 3, 2019, *Forbes*, https://www.forbes.com/sites/nathanvardi/2019/06/03/finance-billionaire-ken-griffins-citadel-securities-trading-firm-is-on-a-silicon-valley-hiring-binge/#34f23c9c6b36 accessed August 2020.

71 Terrance Hendershott, Charles M. Jones, and Albert J. Menkveld, Does Algorithmic Trading Improve Liquidity?, *The Journal of Finance*, Volume 66, No. 1, February 2011, http://faculty.haas.berkeley.edu/hender/Algo.pdf.

72 Jane Croft, "Citadel Securities sues rival over alleged trading strategy leak," *Financial Times*, January 10, 2020, https://www.ft.com/content/2cbf1738-33cd-11ea-9703-eea0cae3f0de accessed December 2020.

in this space could increase the attractiveness of attempting this type of scheme. We ultimately deem it unlikely that a bad actor would seek to use CAT data in this way because of the difficulty in both achieving the hack as well as the effort to reverse engineer an algorithm. The separation and encryption of the Customer and Account Attribute data (in the CAIS database) and trade data (in the MDS database), the fact that the trade data is anonymized, and the limitations on ways in which one can get this data (CAT data can only be accessed by the SEC and SROs via private line access; there is no public internet access and access to the CAIS is on a "need to know" and "least privileged" basis) would make this scenario very difficult to achieve. The hacker would need to successfully access all this data, decrypt it, and reverse engineer the algorithms under which the trades were made. Given the potential value (severity) of this type of information, however, bad actors could be so motivated. In particular, a state sponsored hacker could have the resources to attempt to reverse engineer successful algorithms and steal intellectual property in this way. The bad actor could also seek to ransom the algorithm to the algorithmic trading firm as discussed above or seek to sell the data to a sophisticated trading firm that was able to do the reverse engineering.

An example of a parallel type of scenario can be seen in the breach of newswire services by a group of Ukrainian hackers during 2015. The hackers gained access to corporate earnings releases for dozens of companies as much as 12 hours prior to their being made public. The hackers knew the information was valuable but did not know how to trade based on it. They therefore set up a network of traders to whom they fed the data and either sold them the releases outright or struck a deal to share in the profits.[73] More than $100 million was allegedly earned on the wrongful trades.[74]

In summary, we believe that while the implementing this type of breach would be difficult and the frequency likely low, the severity of a breach leading to the reverse engineering of an algorithmic trading firm's strategy could be high. An estimate of exposure of at least $100 million per incident (based on the cost to develop a successful strategy at Citadel) seems reasonable. Given the role that algorithmic trading firms play in adding liquidity to the markets, we deem this scenario to pose both a risk to algorithmic trading firms themselves, as well as to the efficient operation of U.S. markets. Therefore, we believe this scenario would be very difficult to implement, will occur infrequently, but have extreme severity if successful.

---

[73] See SEC website, "SEC Reaches Settlements with Traders in Newswire Hacking and Trading Scheme," Litigation Release No. 24833, June 10, 2020, https://www.sec.gov/litigation/litreleases/2020/lr24833.htm accessed November 2020. Also see SEC website, "SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases," August 11, 2015, https://www.sec.gov/news/pressrelease/2015-163.html accessed November 2020.

[74] See SEC website, "SEC Reaches Settlements with Traders in Newswire Hacking and Trading Scheme," Litigation Release No. 24833, June 10, 2020, https://www.sec.gov/litigation/litreleases/2020/lr24833.htm accessed November 2020. Also see SEC website, "SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases," August 11, 2015, https://www.sec.gov/news/pressrelease/2015-163.html accessed November 2020.

(4) Fake Data Insertion to Wrongfully Incriminate

We posit that if a hacker were able to successfully insert false data into the CAT, they could use that ability to wrongfully incriminate an individual or company. For example, assume that a hacker inserts data into the CAT making it appear that the CEO of a company was wrongfully engaging in insider trading of its company's stock. Further assume that this data triggered an investigation at the SEC into the CEO's trading and that investigation led to a preliminary injunction hearing to prevent the CEO from further accessing his or her account. This SEC action would be public, and both the CEO's and company's reputation and value could be harmed.

According to a 2010 study, when the SEC announced an investigation on a company, the average abnormal return based on that announcement was at least negative 8%.[75] This would equate to a reduction in market value of $1.8 billion for the median company in the S&P 500.[76]

The negative return can be significantly larger than 8%. In November 2019, the Wall Street Journal announced that the SEC was investigating Under Armour. On the day of the announcement, Under Armour's stock fell 19%.[77] Correspondingly, the market capitalization of Under Armour fell from $9.04 billion to $7.35 billion, a drop of $1.69 billion.[78]

Given the expected negative market reaction to an SEC investigation, the hacker could position to benefit from a stock price drop. This type of trading would arguably be akin to insider trading (trading on material non-public information), where we have seen cases that have generally generated illicit profits ranging in the hundreds of thousands to tens of millions of dollars. The largest insider trading matters to date were Martoma/SAC[79] and Galleon/ Rajaratnam,[80] with alleged wrongful profits of $275 million and $95 million respectively.

---

75 Journal of Forensic & Investigative Accounting, "Market Efficiency and Investor Reactions to SEC Fraud Investigations," Vol. 2, Issue 3, Special Issue, 2010, p. 3.

76 Using the total market value of the S&P 500, $30.24 trillion, a negative 8% return would be a reduction in market value of $1.8 billion for the median company in the S&P 500 (median market value of $22.1 billion). See Refinitiv website, a company that provides financial data, https://www.refinitiv.com/en/about-us accessed October 21, 2020.

77 Wharton University of Pennsylvania, "How Undisclosed SEC Investigations Lead to Insider Trading," March 2, 2020, https://knowledge.wharton.upenn.edu/article/undisclosed-sec-investigations-lead-insider-trading/ accessed September 2020.

78 This market value drop may not be fully attributable to the announcement and would require an event study to test that conclusion. See Refinitiv website, https://www.refinitiv.com/en/about-us.

79 See Final Judgement as to Defendant CR Intrinsic Investors, LLC, United States District Court, Southern District of New York, 12 Civ. 8466 (VM), filed June 18, 2014, p. 3.

80 See Opinion and Order, SEC v. Raj Rajaratnam, et. al., United States District Court, Southern District of New York, 09 Civ. 8811 (JSR), filed November 8, 2011, pp. 1-2.

We recognize that this scenario seems attenuated and unlikely because the hacker would need to know information from the separately kept and encrypted CAIS and trade databases. The hacker would need gain access to the CAIS to obtain which CCID went with the person/company to be wrongfully incriminated. The hacker would then be able to search the trade data for trades related to that CCID. Other potential hacker impediments include CAT data only being accessed by the SEC and SROs via private line access; there is no public internet access and access to the CAIS is on a "need to know" and "least privileged" basis. Additionally, we believe that this false accusation would be relatively easy for the accused CEO to disprove based on simply producing his own account statements. However, this could potentially occur at or after the public injunction hearing, and the associated initial effects on stock price. We conclude that this scenario would be very difficult to implement, will occur infrequently, but have high to extreme severity if successful. The severity level is based on the potential to profit from wrongful accusations about a company and/or its management.

(5) Data Removal or Insertion to Hide Fraud

The SROs and the SEC monitor the securities markets for a range of wrongful activities, such as trading in a way that manipulates the market prices of securities and trading on inside information (material non-public information). If a hacker were to access the CAT and remove data relating to wrongful acts (or insert data to obfuscate their bad acts) and the wrongful acts were not detected by SRO monitoring, the hacker could successfully hide illegal trading activity from regulatory scrutiny. This has the potential to enable illegal activity to continue (and its related profits) and ultimately undermine the efficiency of the markets and public trust therein. Ultimately the investing public is harmed as they may overpay for a purchase or receive less for the sale of a security.

If a bad actor can continue to make millions of dollars on illegal activity due to the insertion of fake data or deletion of data in the CAT, those activities essentially cause those millions to come out of the accounts of investors who are following the rules. To the extent the illegal activity becomes widespread, investors could lose confidence in the market and ultimately take out their money and potentially invest it in foreign markets. This would essentially increase capital costs for all companies seeking to raise funds to grow, translating into a smaller economy.[81]

---

81 "America's historical approach to our capital markets—an approach focused on transparency, materiality, fairness and accountability—has produced a remarkably deep pool of capital with unprecedented participation. It is our Main Street investors and their willingness to entrust their hard-earned money to our capital markets for the long term that have provided the seeds for the deepest, most dynamic and most liquid capital markets in the world. Their capital provides businesses and municipalities with the opportunity to invest, grow and create jobs with an organic dynamism that stands apart both today and since the Commission was formed 85 years ago." See Chairman Jay Clayton, Testimony on "Oversight of the Securities and Exchange Commission" Before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, December 10, 2019, https://www.sec.gov/news/testimony/testimony-clayton-2019-12-10 accessed November 2020.

To execute such a scheme, the bad actor would need to know how to hack into the encrypted and anonymized CAT trade data or hire someone to do so. The bad actor would also have to override or bypass the existence of two separate data feeds into CAT (one from the execution venue and one from the CAT Industry Member reporter) to delete or add fake data or access the final corrected database.[82] Given the potential payoff (severity), such an arrangement between a hacker and a bad actor could occur. For example, and as mentioned above, the SEC charged 32 defendants (primarily based in Ukraine) in a scheme where hackers obtained data from press releases prior to their public release and conspired with experienced traders to trade on earnings announcements based on the hacked data. These acts allegedly occurred over a five-year period and the information from the yet-to-be issued news releases was used to generate more than $100 million in illegal profits.[83] If the trading data relating to these wrongful trades had been deleted, it is likely this scheme would never have been detected and stopped.

This type of criminal trading undermines both market efficiency and public confidence in the markets. The effects may be pernicious and, if left unchecked, could lead to catastrophic loss of investor confidence.

Given the nature of this scheme, including avoiding detection by SRO monitoring, we believe this scenario would be very difficult to implement, will occur infrequently, but have high to extreme severity if successful.

(6) Trading on Non-Public Information

We posit that the non-public trading data in the CAT could be used to determine if a company or individual might be making large multi-day purchases or sales of securities of various companies. This information could indicate a potential takeover, or, in the case of a high-profile investor, a significant new position is being taken.

For example, it is not unusual for Berkshire Hathaway ("Berkshire") to purchase large amounts of stock of a company, and for the stock of that company to go up in value both because of share demand increase based on the size of the purchases made by Berkshire, as well as the perceived value of having Berkshire as an investor once that position is public. Once the position exceeds 5% of the target company, Berkshire (or any investor for that matter) has ten days to report its holding to the SEC.[84] If someone with access to CAT trading data were to see that a significant position was being bought in a particular stock, they could use that information to take a long position in that stock in anticipation of a stock price rise that would occur once that information was made public.

---

82 Data can be accessed by regulators via a query on day one after initial data validation as well as on day 5 when all data has been corrected. See SEC, *Order Approving CAT*, pp. 100 and 538.

83 SEC website, "SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases," August 11, 2015, https://www.sec.gov/news/pressrelease/2015-163.html accessed November 2020.

84 Fintel website, Berkshire Hathaway Inc – Warren Buffet – Activist 13D/13G Filings, https://fintel.io/i13d/berkshire-hathaway. This website contains a list of Berkshire Hathaway SEC 13D/13G filings accessed November 2020.

On November 14, 2016, Berkshire reported to the SEC, with the SEC making it public at 4:05 p.m. ET, a new investment in American Airlines[85] amounting to 4.2% of the stock, or 21,770,555 shares.[86] At this time, American Airlines' stock price was trading around $43.40 per share[87] making the position worth around $945 million. Hypothetically, if someone had been able to front run 10% of these shares and net $1.36 per share (which represents the one day increase in share price post the announcement), the gain would have been $3.0 million.[88]

The hacker also could access the CAT trade data to look for new stock positions being taken in an account in a particular company that approaches 5%. This is referred to as a "toehold" position and could be an indicator that a takeover bid is likely.[89] The hacker could then take a long position in the stock of the target firm to benefit from the takeover announcement, after which stock prices of the target can jump substantially.[90] The hacker would not know with certainty that the entity building the position will continue to make purchases but by pursuing this strategy across multiple examples, they have a high likelihood of success.

---

85 Berkshire's SEC Form 13F filing shows that Berkshire acquired 21,770,555 (13,355,099 plus 8,415,456) shares of American Airlines stock. See SEC's Edgar Website, Berkshire Hathaway Inc filings, https://www.sec.gov/Archives/edgar/data/1067983/000095012316022377/0000950123-16-022377-index.htm, SEC's Edgar website, Berkshire Hathaway Inc filings, https://www.sec.gov/Archives/edgar/data/1067983/000095012316022377/xslForm13F_X01/primary_doc.xml and SEC's Edgar website, Berkshire Hathaway Inc filings, https://www.sec.gov/Archives/edgar/data/1067983/000095012316022377/xslForm13F_X01/form13fInfoTable.xml accessed November 2020.

86 American Airlines had 518,130,000 shares of stock outstanding as of November 14, 2016. See Refinitiv website, https://www.refinitiv.com/en/about-us. 21,770,555 / 518,130,000 = 4.2%.

87 American Airlines stock price closed at $43.40 on November 14, 2016, just prior to the SEC making Berkshire's American Airlines stock acquisition public. See Refinitiv website, https://www.refinitiv.com/en/about-us.

88 21,770,555 shares times 10% times $1.36 = $2,960,795. American Airlines stock price close prior to the announcement was $43.40 (November 14, 2016) and $44.76 after the announcement (November 15, 2016). $44.76 - $43.40 = $1.36. This is an illustration, and we did not perform an event study to determine whether the full price increase is attributable to the announcement.

89 Investopedia website, Toehold Purchase definition, https://www.investopedia.com/terms/t/toeholdpurchase.asp accessed November 2020.

90 Jensen and Ruback (1983) review several empirical papers that empirically estimate the abnormal returns that accrued to the shareholders of the target firms around the announcement dates associated with unexpected tender offers to be approximately 30%. See Jensen and Ruback, "The Market for Corporate Control," Journal of Financial Economics, 11, (1983).

As discussed above, we know hackers are motivated to find and monetize non-public information (earnings announcements hacked from press release services). Such non-public information has also been obtained by hackers on the SEC's company filing website, Edgar. In 2016, bad actors hacked into the SEC's Edgar company filing system to access the data in company filings before the SEC made then public.[91] Such filings include earnings releases and the filings related to stock positions that exceeds 5% of the stock of the company being purchased (discussed above).[92]

In summary, we believe that a hacker could use CAT trade data to successfully trade on non-public information. The payoffs could be high enough to motivate a bad actor. Of course, the hacker would need to gain access to the encrypted and anonymized CAT trade data. If the trade data was obtained, it would be relatively easy to determine if an account was building a position in a particular stock. Thus, we believe this scenario would be relatively less difficult to implement, could occur relatively frequently across multiple stocks, and have medium to high severity if successful.

(7) Competitive Intelligence – Customer Lists

Another possible use of hacked CAT data would be to gather competitive information. A bad actor could hack into the CAT trade data and CAT CAIS data to determine which brokerage firms had which clients. For example, it could be useful to firm A to know that most of a particular pension fund's trading activity is being done at firm B, and how much trading that comprises. With that information, trading firm A could target the most profitable clients and avoid spending time on others. Access to CAT information could notably increase the scope and precision of competitive intelligence above that already available from other, more standard sources.

While this information could provide an advantage, we deem this scenario unlikely. First, as discussed above, there is difficulty in hacking two sources of encrypted and separately kept data, the CAIS (for the account owner associated with the CCID used in the trade database) and trade data as well as associating all of this to learn who the best customers are. Second, merely knowing who is working with whom does not, in and of itself, generate profits; therefore, the incentive to pursue this activity is low. In addition, taking advantage of this information would need to be undertaken by a regulated firm, and if the hacking was uncovered it would lead to severe consequences for that firm. Therefore, the combination of low value of the information and high risk for the user leads us to conclude this scenario is very unlikely. What seems a little more plausible is a bad actor asking the brokerage firm for a ransom and, if not received, the bad actor releasing the information into a public forum. Thus, we believe this scenario would be very difficult to implement, will occur infrequently, and have medium to high severity if successful.

---

91 See NPR website, Barbara Campbell, "SEC Says Cybercriminals Hacked Its Files, May Have Used Secret Data for Trading," September 20, 2017, https://www.npr.org/sections/thetwo-way/2017/09/20/552500948/sec-says-cybercriminals-hacked-its-files-may-have-used-secret-data-for-trading accessed September 2020.

92 See SEC website, https://www.sec.gov/forms accessed September 2020.

(8) Discovery of Regulatory Investigation that Could be Used to Harm Someone's Reputation

It is our understanding that queries made by regulators on the CAT system will be saved, and that the party (e.g., the SEC) making the query will be associated with the query.[93] If a hacker were able to view those queries and also had the Customer and Account Attribute data to identify the firm that is the subject of the query, he or she would be able to determine which firms were under regulatory scrutiny.

This information could be used to ransom the firm as well as purchase or sell securities to take advantage of a potential announcement of an investigation (or a resolution of an investigation) later in time. To accomplish this scheme, the hacker would need to gain access to the queries as well as the encrypted CAIS database (Customer and Account Attribute data). Importantly, access to the CAIS is on a "need to know" and "least privileged" basis and cannot be obtained from public internet connectivity. Additionally, the hacker would not know with certainty that the queries would turn into a publicly announced SEC investigation, but by pursuing this strategy across multiple examples, they have a higher likelihood of success. A hacker with access to the queries would likely need to implement a trading strategy across multiple companies to ensure at least one or more investigations were ultimately disclosed. We conclude this scenario will be of average difficulty to implement, will be of average frequency, and have medium to high severity.

93 See SEC, *Order Approving CAT, The Limited Liability Company Agreement of CAT LLC,* Appendix D-25 to D-27.

E. **Summary**[94]

	Potential Outcomes of CAT Related Cyber Breaches	Relative Difficulty of Implementation	Relative Frequency	Conditional Severity
1	Holding Data Hostage			
	a Threaten to publicly release confidential Customer and Account Attribute data or trade data to harm a firm's or investor's reputation	Medium	Low	Low to Medium
	b Threaten to keep data encrypted (denial of service) to prevent its use by regulators	Medium	Low	Low to Medium
	c Threaten to sell trading data regarding an account that could allow reverse engineering a trading algorithm	High	Low	High to Extreme
	d Threaten to make short position data public	Medium	Low	Medium
2	Identify Theft	Low	Medium	Medium to High
3	Algorithm Reverse Engineering	High	Low	Extreme
4	Fake Data Insertion to Wrongfully Incriminate	High	Low	High to Extreme
5	Data Removal or Insertion to Hide Fraud	High	Low	High to Extreme
6	Trading on Non-Public Information	Low	Medium to High	Medium to High
7	Competitive Intelligence - Customer Lists	High	Low	Medium to High
8	Discovery of Regulatory Investigation that Could be Used to harm Someone's Reputation	Medium	Medium	Medium to High

III. Economic and Public Policy Analysis of Cyber Security for CAT LLC

In this section, we review the law and economics literature that provides normative analysis of whether the preferred method to influence the management of risky activities is via regulation or litigation. Our goal is to apply the lessons from this literature 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. We start by providing a rationale for why one would want to influence the loss-producing behavior of economic agents. We then characterize the differences between regulation as an *ex-ante* method of exercising control versus litigation as a method that influences behaviors before the loss-producing event occurs by assigning liability *ex*

[94] See discussion in Section D for an explanation of each column.

post. The discussion proceeds by comparing the relative advantages of disadvantages of each method, contrasting one relative to the other.

In reviewing CAT LLC's proposed plan amendment for a limitation of liability, the Commission is faced with the choice of whether to supplement the cyber regulatory regime that the Commission has already imposed by affording Industry Members the ability to bring private litigation against CAT LLC and the Participants. Based on our application of the economic literature, we conclude that regulation alone is preferable to regulation plus litigation. As discussed below, the approach that relies largely on regulation alone would be an improvement in economic efficiency and a benefit to the investing public over a regulation plus litigation approach as proposed by Industry Members. Accordingly, the limitation on liability proposed by the Participants is appropriate from the perspective of economic theory.

A. The Choice Between Regulation and Litigation

The standard (legal, economic, and moral) reason for seeking to control the actions of economic agents who engage in risky activities is to maximize the social welfare of the activity. Steven Shavell, the Samuel R. Rosenthal Professor of Law and Economics at Harvard Law School, provides a useful definition of social welfare as "the benefits [each] party derives from engaging in their activities, less the sum of the costs of precautions, the harms done, and the administrative expenses associated with the means of social control."[95]

Regulation is one of the primary "means of social control" referenced in Shavell's definition. Regulatory control is characterized by its reliance upon rules designed to reduce to some acceptable level the likelihood of occurrence of a loss, or to minimize the size of the loss, should one occur. These rules are most often defined by professionals who are experts in the underlying risk exposure, and they are promulgated before the economic activity commences. Each party to the activity is required to follow the rules and enforcement is typically conducted using publicly observable mechanisms.

Litigation is a second "means of social control." Economists (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. Litigation is characterized by the use of legal standards to assign liability after the loss producing event has occurred that are applied and adjudicated by non-experts in the underlying risk using private enforcement mechanisms (e.g., civil lawsuits involving private lawyers, judges and jurors) that may involve informing the non-experts using testimony provided by experts (i.e., by expert witnesses, professionals, etc.).

One-way economists examine which method of social control may be preferable is in the context of "incentive alignment" among the parties to the economic activity. That is, how do you get each party to recognize and address not only the damages they might suffer, but the damages that other parties (customers, vendors, employees, etc.) might incur because the first party suffered an adverse event?

---

95 Steven Shavell, "Liability for Harm Versus Regulation of Safety," *The Journal of Legal Studies*, Vol. 13, No.2 (June 1984), pp. 357-374.

We focus on comparing regulation vs. litigation and on systems of social control that employ the joint use of each tool for the purposes of this White Paper.

B. Economic Determinants of the Relative Attractiveness of Regulation or Litigation to Control Risk

A well-established literature has developed over several decades that discusses the circumstances when regulation or litigation will be the preferred means of control to minimize the social cost of loss producing events.[96] This subsection examines general economic considerations underlying a mix of regulation and litigation that minimizes the overall expected costs of adverse events such as cyber breaches. Subsequently, we apply the insights of this literature to the issue at hand – the optimal control of cyber risk for CAT LLC, and whether the Commission should supplement the existing regulatory regime by allowing Industry Members to sue CAT LLC and the Participants in the event of a breach.

A first consideration relates to the rules-based nature of regulation. Regulation relies upon each party having a clear understanding of the legal obligation they must perform before they conduct the economic activity. Regulation tends to be preferred to litigation in circumstances where the rules can be written with precision, when the marginal compliance costs associated with the rules are low, and when compliance can be transparently verified by all parties, including the first party, all third parties, and by the regulator.[97]

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.

---

96 In addition to the 1984 Shavell article referenced in the prior footnote, the following articles are of particular note: Ronald H. Coase, "The Problem of Social Cost," *Journal of Law and Economics,* Vol 3 (1960), pp. 1-44; Harold Demsetz, "When Does the Rule of Liability Matter?" *Journal of Legal Studies,* Vol. 1, No. 1, (January 1972) pp. 13-28; and Steven Shavell, "Liability for Accidents," Chapter 2 in *Handbook of Law and Economics, Vol. 1,* Mitchell Polinsky and Steven Shavell, eds., Elsevier, 2007. There are many additional references in the latter chapter.

97 The compliance transparency condition is complicated in the case of cyber security by the need to prevent cyber criminals from understanding and evading cyber defenses and by the fact that cyber criminals themselves operate with great secrecy to avoid detection. A litigation approach, however, offers no advantage over regulation in compliance transparency and may actually increase the risk of cybercrime elsewhere by inadvertently disclosing information on cyber defenses. It is also germane to note that Industry Members sit on the Advisory Committee and SEC representatives have substantial visibility into the operations of the CAT and the Plan Processor. We discuss this latter point in detail later in the White Paper.

Regulatory rules that cannot be precisely written are also problematic to the extent they cause the parties to the activity to inadvertently not follow the rule or to have different interpretations of the rule. In either circumstance, it may be possible that all parties incur the administrative costs of designing the rule and of attempting to comply with the vague rule, and then also incur the administrative costs associated with interpreting the application of the vague rule once the loss has occurred. This duplication of administrative costs, both *ex-ante* and *ex post*, reduces the attractiveness of regulation in favor of litigation where the administrative costs are borne only once.

Regulatory systems tend to dominate when compliance with the rule(s) can be monitored by the regulator with low marginal cost and there is high transparency regarding the effort taken to comply with the rules. Litigation dominates in situations when there are significant informational asymmetries between the parties or between the parties and the regulator to determine compliance. The adversarial nature of proceedings where courts can compel the parties to reveal private case-specific information that has already taken place leads to more accurate liability assignment *ex post* and, therefore, incentives to mitigate the risk *ex-ante*. As a result, a litigation regime provides stronger incentives for each party to internalize the private information they have about the effort they take to minimize losses about the damages they might suffer, or about the damages they might impose on the third party relative in situations where it is costly for the parties to become informed about each other's actions *ex-ante* or in real-time.

Regulatory systems are preferable when the activity can result in so-called "judgment proof problems." A judgment proof problem is synonymous with the classic externality where the actions of a responsible party imposes costs on a third party (or parties) that the responsible party is unable or unlikely to pay despite being the source of those costs. Agents can be judgement proof for several reasons. A responsible party may be judgment proof if the losses it produces are spread amongst many third parties and no single entity has a large enough incentive to hold the first party accountable for the damages it produced – the so-called "disappearing defendant" problem. A responsible party may also be judgment proof when the adverse event produces a catastrophic loss that exceeds the first party's available assets to provide compensation. Litigation systems, by definition, allow for the possibility that the catastrophic loss may happen and thereby permit the prospect that full recovery by the injured party may not be possible. Knowing the effects of a possible catastrophic event will not be fully realized by the first party reduces the first party's up-front incentives to take care.

The *ex-ante* approach of regulation mitigates judgement proof problems by seeking to avoid the loss itself. Appropriately designed, regulations can compel the first party to internalize expected social costs of losses suffered by third parties, incorporating those third-party costs into the first-party's decision making.

It is also important to consider the joint use of each policy tool. For example, drug manufacturers are subject to testing regimes (*ex-ante* regulation) before a new drug can be licensed and sold on the market and can be held liable for damages (*ex post* litigation) for drugs that cause injury to consumers, sometimes even in cases where the manufacturer followed all the up-front testing regimes.

From an economic perspective, the joint use of both regulation and litigation should be considered only when there is sufficient incremental efficiency that can be gained by using both methods of social control collectively. In these situations, one method – either or regulation or litigation – will be the primary method, and the relevant question is whether adding the other method will improve incremental efficiency. For example, an article in the leading economics journal argues litigation supplemented by regulation can resolve a form a judgment proof problem that arises when it is possible a third party may be unable to recover damages because courts can make errors by incorrectly applying a negligence standard. Adding regulation, *ex-ante*, to the *ex post* liability regime can help mitigate the litigation uncertainty by ensuring the negligence standard established by the court is not too low.[98]

Similarly, there are circumstances where it is advantageous to add litigation to mitigate the informational limitations of the regulatory policy tool. For example, the efficacy of regulation declines when a regulator monitoring a firm can observe compliance with certain rules but not others. In this case, adding liability through litigation to the regulatory regime can increase the efficiency of the entire system because *ex post* litigation is better suited to consider context-specific information after the loss has occurred focused on the rules for which compliance cannot easily be verified *ex-ante*.[99] A second area where regulatory systems suffer is when the regulator faces differential ability to monitor the firms in the industry it is overseeing or the firms have heterogenous assets such that it is difficult to write precise rules and standards. Both circumstances can create *ex post* judgement proof problems. In this case, using a regulation approach with relatively low compliance standards helps to avoid some of the losses while adding the liability regime can serve to provide additional incentives to mitigate the risks that are tailored to the specific circumstances of the individual loss-producing entity.[100]

Financial services and health and safety are two areas where the informational limitations and differential ability to monitor has corroborated the co-existence of regulation and litigation as means of *ex-ante* risk control. Financial institutions, for example, are regulated regarding the risk they might pose in the areas of solvency and consumer disclosure. But they are still subject to litigation over specific transactions where the information requirements to make certain decisions are high. We see similar strategies employed in the food and drug industries. There exist baseline regulatory requirements, but harmed parties are still permitted to sue based on specific circumstances giving rise to their harm.

The CAT is different from the examples cited here that support the co-existence of regulation and litigation to control risky behavior. The CAT does not face numerous customers with different fact-specific conditions. There are a relatively small handful of parties involved,

---

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

99 Bhole, Bharat, and Jeffrey Wagner, "The Joint Use of Regulation and Strict Liability with Multidimensional Care and Uncertain Conviction," *International Review of Law and Economics* Vol. 28 (2008) pp. 123-132.

100 De Geest, Gerrit, Giusseppe Dari-Mattiacci, "Soft Regulators, Tough Judges," *Supreme Court Economic Review* Vol. 15 (2007) pp. 119–140.

all of whom are already regulated by the SEC. 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.[101] The Industry Members, even though they do not run the day-to-day operations of CAT, have the opportunity to comment on this proposal (as they do with all proposed CAT NMS Plan amendments). Similarly, in May 2020 the SEC amended the CAT NMS Plan with the goal of increasing operational transparency and financial accountability.[102]

The SEC can also file enforcement actions to compel compliance with the extensive cyber security requirements for the CAT. Enforcement action brought by the SEC against the CAT would be highly informed by the SEC's pre-existing regulatory supervision and is potentially informed by Industry Members through their ability to monitor CAT via their role on the Advisory Committee. The SEC, therefore, 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. The SEC is also able to use information that it acquires through multiple sources including its own examinations and, potentially, investigations of the CAT in conducting that cost-benefit analysis.

The litigation ability sought by Industry Members, however, is of a substantially different nature than that held by the SEC. The possibility of the CAT being forced by Industry Member initiated litigation to take actions either in conflict with or uncoordinated with the SEC's regulatory requirements is not trivial.[103] Furthermore, adding litigation to regulation does not resolve judgement proof problems, and in fact, for some judgment proof problems, it may not be the preferred solution.

Shavell suggests compulsory insurance is a potential solution to the judgment proof problem of inadequate assets as a way to compensate injured victims.[104] He cautions, however, the problem of inadequate assets that leads to inadequate incentives to take care will not be ameliorated if the insurer is unable to design an insurance contract where the insurance premium

---

101 For a recent proposal, see SEC, *Amendments to the National Market System Plan Governing the Consolidated Audit Trail to Enhance Data Security*, RIN 3235-AM62, Release No. 34-89632, File No. S7-10-20, August 21, 2020.

102 SEC, *Amendments to the National Market System Plan Governing the Consolidated Audit Trail*, RIN 3235-AM60, Release No. 34-88890, File No. S7-13-19, May 15, 2020.

103 Litigation on the part of Industry Members, if successful, could result in a court decision that addresses one type of risk but then distorts cyber hygiene for the CAT away from other, now more pressing risks. The court decision, by its nature, remediates past problems with little, or no, regard to the problems arising in the future. A litigated solution could address a particular risk, but then inhibit the adoption of newer cyber hygiene methods.

104 Shavell, Steven, "The Judgement Proof Problem," *International Review of Law and Economics* Vol. 6, No. 1 (June 1 1986), pp. 45-48.

reflects the insurer's ability to monitor the insured's readiness (the premium recognizes investments by the policyholder to reduce the likelihood of loss), if the insurance is only available at limits well below the potential loss, or if the insurance is priced above the actuarially fair premium.

C. Special Considerations Arising for the CAT's Cyber Security

There are certain special considerations when examining the roles of regulation and litigation in aligning incentives appropriately for CAT's cyber risk. While regulation has a long history in public policy towards economic activity, cyber risk presents features that transcend prior regulatory endeavors. Much of regulation, for example, addresses relations between regulated entities and their customers or vendors – parties that enter into legal transactions willingly. Health and safety regulation, as another example, focuses on decisions and actions that are solely under the control of the regulated entities. Safety regulation of nuclear power plants, for example, is designed to avoid accidents that would create considerable harm to those living within the vicinity of the plant but for which there does not exist a contractual relationship between the parties.

The question of how best to encourage investment in protection against cybercrime is challenging because the parties harmed are varied, there exist circumstances where it may not immediately be known that a loss has occurred, and holding the perpetrators liable for their actions, even if they can be identified, is often not possible. On a very general level, entities that may be targets of cybercriminals have incentives to invest in cyber security measures up to the point where the last dollar of expenditures is expected to prevent at least that level of cyber loss to the entity. Cyber losses consist of direct costs to the breached entity and the costs that the entity expects it would pay to other parties harmed by the entity's cyber breach. The concern, therefore, is that entities may choose to not invest at a socially optimal level of protection if they do not internalize the expected direct costs of the potentially breached entity as well as the costs of all other affected parties. System administrators who have the responsibility to maintain and enhance the integrity of information assets and the systems that protect them may face situations where the benefits that might accrue from an investment in security may accrue to others outside the firm but may not be fully internalized to the firm. In these cases, markets do not provide sufficient incentive for the optimal investment in protection. Without an intervention of some sort to correct the externality, such as the cyber security regulatory regime mandated by the SEC, there may be insufficient incentive to invest in security at the economically optimal level.

Regulation of cyber security adds an additional dimension that is novel and difficult to manage – protection against malicious actors that have incentives and abilities to wreak havoc against parties with whom they have no consensual relationship while simultaneously avoiding legal sanction. Importantly, litigation against the first-party breach victims by third-party victims of cybercrime adds little, if any, incentive or ability to mitigate the frequency or severity of cybercrime when the first party is subject to an extensive, transparent, and well-functioning regulatory approach to overseeing cyber security.

For the reasons discussed in Section II, possible cyber breaches of the CAT can cause the CAT, the Plan Processor, and the Participants themselves to all experience significant harm (e.g., loss of data or access to regulatory capabilities). The adverse effects on this group as first-party operators are already incorporated into the decisions the CAT and the Plan Processor regarding

cyber security. Moreover given the fact that: the SEC is another party affected by the CAT's cyber risk, the Plan Processor is required to comply with the SEC's cyber mandates, and the Industry Member's role on the Advisory Committee,[105] there is little, if any, additional harm to third parties that is not already incorporated into the decision making of the CAT and the Plan Processor. In economic terms, adding the threat of litigation would do nothing to further internalize into the CAT's decision making the possible losses suffered by the Industry Members. Indeed, it is possible that efforts to reduce the cyber risks that most concern Industry Members in an effort to avoid litigation may take resources from the CAT that would be better used to improve overall cyber hygiene.

Another notable information asymmetry in the cyber security arena is the ability of perpetrators to hide methods, intentions, and targets from scrutiny. Even with diligent cyber security efforts on the part of potential targets, cyber breaches may not be detected promptly enough, and first-party breach victims may not know they have been breached. Even though there are now extensive breach notification requirements (including in the CAT NMS Plan), it takes time and effort to understand the scope of the breach and the scale of the required notifications. Relatedly, breached entities may have incentives to not reveal they have been hacked. Cyber breaches occur often because of weaknesses in software design and implementation that are then exploited by the bad actors. Relevant software is most often purchased from non-parties and affected parties rely on the integrity of the purchased software. There is also a public goods nature for information about cyber breaches. Knowledge of a particular cyber breach at one victim can help other targets avoid becoming victims. The incentive to disclose a breach to support others for no private gain is a classic common goods problem.

The concerns about disclosing a cyber breach with the CAT are substantially, if not completely, mitigated. CAT LLC exists only because of an SEC mandate that a centralized database is essential to improving the monitoring and supervision of U.S. securities trading activity. The SEC has closely supervised the formation and operation of the CAT, and there are no other entities similar to the CAT to diffuse the SEC's attention. The SEC has imposed extensive and specific requirements on the CAT regarding its cyber security operations. "The security and confidentiality of CAT Data has been – and continues to be – a top priority of the Commission. The CAT NMS Plan approved by the Commission already sets forth a number of requirements regarding the security and confidentiality of CAT Data."[106] Numerous SEC personnel and regulatory personnel at the Participants will access the CAT's Central Repository

---

105 "Members of the Advisory Committee shall have the right to attend meetings of the Operating Committee or any Subcommittee, to receive information concerning the operation of the Central Repository (subject to Section 4.13(e)), and to submit their views to the Operating Committee or any Subcommittee on matters pursuant to this Agreement prior to a decision by the Operating Committee on such matters. . . ."
See SEC, *Order Approving CAT, The Limited Liability Company Agreement of CAT LLC,* Section 4.13(d).

106 SEC, *Amendments to the National Market System Plan Governing the Consolidated Audit Trail to Enhance Data Security,* RIN 3235-AM62, Release No. 34-89632, File No. S7-10-20, August 21, 2020, I. Background, pp. 9-10.

on a daily basis. The SEC's knowledge of the CAT's cyber security standards and operations is extensive and precise. Finally, CAT is a not a for-profit entity and its fundamental mission is to serve the public good as defined by the SEC. As a result, its incentives to withhold information are minimized relative to for-profit entities.

These considerations present challenging obstacles to an effective litigation approach to cyber security for the CAT. An advantage of the regulatory approach to the CAT's cyber security is the ability of the SEC to require the CAT and the Plan Processor to implement cyber security initiatives, standards, policies, and procedures promulgated by entities with deep knowledge and experience in cyber matters—thereby internalizing the social benefits of investing in cyber security into their decision making. The 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.[107] An SEC enforcement action (litigation) would likely be settled with the non-complying party(ies). This has the benefit of penalizing non-compliance without the added cost of protracted litigation. Adding a third-party litigation approach as proposed by Industry Members on top of existing regulation and potential enforcement action runs the risk of incurring marginal costs without adding any incremental benefit. We elaborate on this point in Section D.2 below.

D. Assessment of Regulation and Litigation Approaches as Applied to a Potential CAT LLC Cyber Breach

In this section, we apply the economic considerations discussed in Sections A through C above to analyze whether CAT's cyber security risk should be addressed through regulation, litigation, or a combination of both methods. We conclude that affording Industry Members the ability to sue CAT LLC and the Participants for damages suffered as a result of a potential CAT data breach would not meaningfully increase the incentives for CAT LLC to take appropriate cyber precautions but would increase the costs to various market participants, including the Participants, Industry Members, and individual investors. Under these circumstances, the Participants' proposed limitation of liability amendment to the CAT Reporter Agreement would serve important policy goals.

1. Recapitulation of CAT's Risks, Standards, Policies, and Practices

The potential for cyber breaches at the CAT exists and can result in harm to some parties is acknowledged by all, including the SEC. "The Commission acknowledges that the costs of a

---

107 Regulation SCI (Regulation Systems Compliance and Integrity and Form SCI) was adopted by the SEC in November 2014 "to strengthen the technology infrastructure of the U.S. securities markets." Regulation SCI applies to the Participants and is designed to "Reduce the occurrence of systems issues; Improve resiliency when systems problems do occur; [and] Enhance the Commission's oversight and enforcement of securities market technology infrastructure." See SEC website, "Spotlight on Regulation SCI," https://www.sec.gov/spotlight/regulation-sci.shtml accessed November 2020.

breach, including breach management, could be quite high, especially during periods of market stress. Furthermore, the Commission understands that a breach could seriously harm not only investors and institutions but also the broader financial markets."[108] In its *Order Approving CAT*, the SEC "explained its belief that it is difficult to form reliable economic expectations for the costs of security breaches"[109] and that "the form of the direct costs resulting from a security breach will vary across market participants and could be significant."[110] The SEC continued, "The Commission is unable to provide quantitative estimates of those costs because there are few examples of security breaches analogous to the type that could occur under the Plan and because the Plan Processor has some discretion in developing its breach management plan."[111]

The SEC has mandated that the CAT and the Plan Processor (FINRA CAT) implement a number of specific cyber security protocols.[112] The SEC's regulation of the CAT, therefore, focuses appropriately on *ex-ante* risk reduction requiring a variety of cyber best practices by the CAT and its users.

The SEC can employ a variety of regulatory enforcement measures to compel the CAT (and other market participants) to establish and maintain a high level of cyber security. With these and other protocols, practices, and procedures in place, "[t]he Commission discussed . . . its belief that the risks of a security breach may not be significant because certain provisions of Rule 613 and the CAT NMS Plan appear reasonably designed to mitigate these risks."[113] In its *Order Approving CAT*, the SEC anticipated and resolved many of SIFMA's concerns regarding the public interest aspect of the proposed CAT Report Agreement amendment.[114] It is worth quoting

---

108 SEC, *Order Approving CAT*, Section V.F.4. *Economic Analysis, Expected Costs of Security Breaches*, p. 708.

109 SEC, *Order Approving CAT*, Section V.F.4. *Economic Analysis, Expected Costs of Security Breaches*, p. 704.

110 SEC, *Order Approving CAT*, Section V.F.4. *Economic Analysis, Expected Costs of Security Breaches*, p. 705.

111 SEC, *Order Approving CAT*, Section V.F.4. *Economic Analysis, Expected Costs of Security Breaches*, p. 708.

112 Consolidated Audit Trail website, Security: FAQs, https://www.catnmsplan.com/faq. Response to questions S1, S10, and S11 accessed August 2020.

113 SEC, *Order Approving CAT*, Section V.F.4. *Economic Analysis, Expected Costs of Security Breaches*, p. 708.

114 *The Commission notes that the Participants' proposed governance structure—with both an Operating Committee and an Advisory Committee—is similar to the governance structure used today by other NMS plans, and the Commission believes that this general structure is reasonably designed to allow the Participants to fulfill their regulatory obligations and, at the same time, provide an opportunity for meaningful input from the industry and other stakeholders.*
SEC, *Order Approving CAT*, Section IV.B.1, pp. 139-140, emphasis added.

extensively from the SEC's *Discussion and Commission Findings* section in the *Order Approving CAT* to understand the approach adopted by the SEC.

> *Rule 613 tasks the Participants with the responsibility to develop a CAT NMS Plan that achieves the goals set forth by the Commission. Because the Participants will be more directly responsible for the implementation of the CAT NMS Plan, in the Commission's view, it is appropriate that they make the judgment as to how to obtain the benefits of a consolidated audit trail in a way that is practicable and cost-effective in the first instance. The Commission's review of an NMS plan is governed by Rule 608 and, under that rule, approval is conditioned upon a finding that the proposed plan is "necessary or appropriate in the public interest, for the protection of investors and the maintenance of fair and orderly markets, to remove impediments to, and perfect the mechanism of, a national market system, or otherwise in furtherance of the purposes of the Act." Further, Rule 608 provides the Commission with the authority to approve an NMS plan, "with such changes or subject to such conditions as the Commission may deem necessary or appropriate." In reviewing the policy choices made by the Participants in developing the CAT NMS Plan, the Commission has sought to ensure that they are supported by an adequate rationale, do not call into question the Plan's satisfaction of the approval standard in Rule 608, and reasonably achieve the benefits of a consolidated audit trail without imposing unnecessary burdens. In addition, because of the evolving nature of the data captured by the CAT and the technology used, as well as the number of decisions still to be made in the process of implementing the CAT NMS Plan, the Commission has paid particular attention to the structures in place to guide decision-making going forward. These include the governance of the Company, the provisions made for Commission and other oversight, the standards established, and the development milestones provided for in the Plan.*[115]

The SEC, therefore, after an extensive consideration of the overall costs and benefits of the CAT, already has expressed its judgment that the cyber security requirements it imposed on the CAT sufficiently serve the public interest. In its November 15, 2016 *Joint Industry Plan; Order Approving the National Market System Plan Governing the Consolidated Audit Trail, Supplementary Information*, the SEC concluded, "[T]hat the [CAT NMS] Plan, as amended, is necessary and appropriate in the public interest, for the protection of investors and the maintenance of fair and orderly markets, to remove impediments to, and perfect the mechanism of a national market system, or is otherwise in furtherance of the purposes of the [Securities Exchange] Act [of 1934]."[116]

2. Alignment of Incentives

As explained in Sections A through C above, and mentioned in SIFMA's *Memorandum of Law*, the issue here is the "allocation of risk (and resulting incentives) relating to a potential

---

115 SEC, *Order Approving CAT,* Section IV., *Discussion and Commission Findings*, pp. 126-127, emphasis added, internal footnotes omitted.

116 SEC, *Order Approving CAT,* Section I. *Introduction,* p. 8, emphasis added. Nearly identical wording was repeated in Section IV. *Discussion and Commission Findings*, p. 129 and Section VII. *Conclusion,* p. 979.

CAT data breach to ensure that data is not misused, misappropriated or lost."[117] Industry Members, through SIFMA, assert that the Participants' proposed limitation on liability would impose significant burdens on them. In essence, by advocating against the inclusion of a limitation of liability provision in the Reporter Agreement, Industry Members have argued that the risks associated with a CAT cyber breach are best addressed through litigation they can initiate as opposed to regulation and, if necessary, enforcement action by the SEC. But an application of the economic principles discussed above to an examination of the CAT fundamentally challenges Industry Members' interpretation.

Relying primarily upon a regulatory regime, as proposed by Participants, is reasonable based upon our analysis for several reasons.

- CAT LLC is a legal entity jointly owned by the Participants. The Participants, as SROs, are already overseen by the SEC and are therefore subject to significant regulatory requirements to limit their exposure to cyber risk. The SROs also use the CAT to fulfill their regulatory functions under supervision of the SEC. A cyber breach at the CAT would affect the SROs' ability to perform their regulatory function — meaning that the SROs, as users of the CAT, have a strong interest in the CAT's cyber security. As discussed above, the SEC can impose—and has in fact imposed—additional cyber regulations in response to subsequent developments or to address newly identified threats. As meaningfully regulated entities, the Participants are obligated to comply with regulatory requirements or face consequences. The Participants have already implemented cyber security standards, policies and procedures to protect their information from successful attack. Further, similar to the CAT, SROs have in place liability limitations with Industry Members for cyber loss.[118] If Industry Members have already accepted limitations on liability for cyber loss with individual SROs, imposing limitations on liability for cyber loss applied to an SEC-mandated consortium composed of those individual SROs substantially works to negate the pre-existing individual limitations on liability.
- CAT LLC's funding principles seek to cover the annual operating costs of the company, and the financial assets are designed to be minimal and substantially lower than the maximum possible loss due to several extreme possible cyber breach scenarios. There is presently no asset reserve, and no plans to build one, on the balance sheet of CAT LLC that could cover a substantial cyber loss. Dispensing with the liability exposure will, therefore, not likely change CAT LLC's incentive to avoid losses beyond its existing minimal asset base.
- The efficiency of regulatory systems to achieve economically optimal outcomes declines when the monitor is required to oversee an industry consisting of heterogeneous firms where it is difficult to promulgate rules that apply with equal precision to all firms. As discussed in Section B above, efficiency gains may be

---

117 *Memorandum of Law in Support of SIFMA's Motion to Stay SRO Action Pending Commission Review of SIFMA's Application Pursuant to Exchange Act Sections 19(d) and 19(f)*, April 22, 2020, p. 15.

118 See the discussion in Section 4 for some useful examples.

possible in such an industry by supplementing the regulatory system with a liability system that can add context-specific information should a loss occur. In this case, however, CAT LLC is the only firm being overseen. As a result, the regulatory system is tailored specifically on an *ex-ante* basis with rules targeted to this particular firm. Thus, adding litigation initiated by Industry Members in this case, where context specific information can be considered *ex post,* is difficult to justify as there is an ongoing dialogue where the regulatory rules can be revised and tailored as circumstances change over time through the monitoring mechanisms available to the Industry Members and to the SEC through its examination of the CAT by the Office of Compliance Inspections and Examinations.

- Regulatory arrangements can also be enhanced in situations where the monitoring costs associated with compliance are high and when the regulated activity is composed of heterogenous firms. Again, this circumstance is unique, however, as CAT LLC is the only firm being monitored. Importantly, representatives of the SEC attend all Operating Committee meetings, participate in the Security Working Group and Interpretations Working Group, and receive updates regarding various aspects of the project and system on a daily basis. 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. The Industry Members' role on the Advisory Committee also provides them an ability to attend all Operating Committee meetings as well as meetings of other subcommittees and working groups and, therefore, the ability to advocate for their interests on the cyber security policy and procedures and other issues related to CAT LLC. While the Industry Members' role is advisory in nature, there is no restriction that prevents any Industry Member from raising specific concerns regarding CAT LLC's cyber security directly with the SEC. In addition, Industry Members transfer large amounts of data into the CAT, thereby contributing to the risk of a breach (e.g., malicious data could be inserted, knowingly or not, through an Industry Member data upload). Thus, Industry Members are active participants in the cyber mitigation activities of CAT LLC and active enforcement monitors of the Plan Processor and the Participants.

The SEC has required that CAT LLC and the Plan Processor implement and maintain an extensive cyber security regimen. Importantly, both the SEC and Industry Members can monitor and provide input on the cyber security hygiene of the CAT and the Plan Processor, and the SEC can bring enforcement actions against the Participants if they fail to meet the standards in the regulatory regime. Under these conditions, adding an ability for Industry Members to sue CAT LLC or the Plan Processor in the event of a cyber breach will not meaningfully improve the incentives to implement and maintain the security of the data residing at CAT. Those incentives already exist based on *ex-ante* regulation. Consequently, our analysis suggests removing the limitation of liability provision will not lead to increases in the safety of the cyber security program or reductions in expected losses due to successful cyber-attacks.

3. Additional Costs of Litigation

In addition to considering the potential benefits of litigation (which appear to be minimal for the reasons discussed above), an economic analysis must also consider costs of allowing litigation by Industry Members.

At a minimum, any means of social control of a risky activity comes with administrative expense. It is important, therefore, to determine if the incremental control that comes with the associated set of benefits justifies the additional expense. The additional costs of cyber security protection or remediation (or of compensation paid to adversely affected parties who successfully litigate should a loss occur) that would be funded by CAT LLC need to be examined relative to the expected marginal benefits.

More substantively, the threat of litigation without concomitant benefits can lead to significant extra-marginal costs that reduce social welfare. For example, the threat of medical malpractice litigation has been cited as a motivation for excess medical testing.[119] In this case, the prospect of litigation arising from the absence of the limitation on liability provision has the prospect for prompting overpayment for cyber security on the part of the CAT and the Plan Processor beyond the economically optimal level of protection, despite the analysis we present above suggesting that such litigation would provide no incremental benefit. The prospect of third-party litigation may prompt CAT LLC to expend resources on cyber security systems that supplement the detailed (and regularly updated) framework implemented by the Commission, but that do not reduce the cyber risk commensurate with the costs. The threat of litigation from Industry Members arising from a cyber breach at the CAT could also affect decisions on the implementation of new protocols at CAT. One can easily imagine the Plan Processor, responding to perceived concerns from Industry Members, might adopt an overly risk averse posture and not pursue new opportunities to decrease costs or increase efficiencies at the CAT as new technologies become available given an overemphasis on certain courses of action and underinvestment in others. It could actually result in an overinvestment in cyber security and an underinvestment in productivity-enhancing projects where the costs of these decisions would ultimately be passed on to the investors in the form of higher costs of trading, higher costs of securing capital, etc.

An over-investment in cyber security, moreover, could make the CAT less effective in achieving the Commission's goals. A CAT system burdened by excess security measures could slow down database searches, surveillance programs, and other essential functions. Security measures added to hedge against litigation risk, for example, might limit the number of records that could be returned in a single query, restrict access to a less-than-optimal pool of regulatory personnel (at the SEC and the SROs), or require importation of outside data into CAT environments that would expand the CAT's overall attack surface. Indeed, as noted above,

---

119 By one estimate, Mello, Chandra, Gawande, and Studdert (2010) suggest between 2-3 percent of health care spending in the United States, or $55.6 billion (in 2008), is related to the costs of defensive medicine. See Mello, Michelle M., Amitabh Chandra, Atul A. Gawande, and David M. Studdert, "National Costs of the Medical Liability System," *Health Affairs* Vol. 8, No. 29 (Sep. 2010) pp. 1569-1577.

allowing third-party litigation would run the risk that a court would mandate security protocols that conflict or interfere with those adopted by the SEC.

Extending the CAT's asset base (i.e., increasing CAT LLC's assets or broadening the number of firms potentially liable in the event of a loss) may have the theoretical advantages of reducing the judgment proof problem discussed earlier and provide compensation to those negatively impacted by a cyber event. However, as conceived, CAT LLC is run on a cost-only basis, so there is currently no mechanism to establish safety reserves that might allow the it to build up a cash to pre-fund losses from a cyber breach. One could imagine adopting an alternative funding principle that would permit those harmed by a cyber loss to seek compensation from a fund that could be established on the CAT's balance sheet. Policies and procedures could be developed that would prescribe the source that would finance the fund, that would describe how those funds would be invested, that would define a covered loss, that promulgate how approved claims would be settled, etc.

Although building a pool of capital in this manner might provide some level of compensation to a few entities who could suffer a loss supplying the CAT with the required information, we caution that this course of action has notable possible disadvantages. Beyond the administrative expenses associated with establishing such a business function within CAT, there are well known challenges associated with creating a largely unencumbered pool of capital within organizations as there is considerable evidence doing so can lead to substantially misaligned incentives between managers and the providers of that capital that ultimately lead to significant costs.[120] We provide several alternative ways that would allow the CAT to pre-fund cyber losses in Section E below that we judge would lead to substantially better outcomes than establishing a cyber loss pool on CAT LLC's own balance sheet.

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.

We identified several marginal operating costs that would likely emanate (with no corresponding marginal benefits) if the limitation of liability provision were eliminated. These extra costs are either associated with inefficient litigation, 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 who would ultimately pass those higher costs on to

---

120 See Jensen, Michael, "Agency Costs of Free Cash Flow, Corporate Finance, and Takeovers," *American Economic Review*, Vol. 76, No. 2 (May 1986) pp. 323–329. If the capital pool exists within regulated entities, that, at least potentially, raises additional complications. See, for example, the regulation of insurance company general accounts.

their customers, employees or owners. Research on the incidence of extra-marginal costs and taxes on organizations generally shows that these higher costs tend to fall on employees and customers rather than the owners of the organization.[121] The Industry Members' desire to dispense with the limitation of liability provision may, at best, result in avoiding some losses or, possibly, providing compensation for cyber breaches to a handful of Industry Members and their clients. But our analysis suggests the costs will likely be far higher and spread throughout the system as a whole, likely leading to reduced trading levels, reduced participation in markets by investors, or increased costs of raising capital. Moreover, since any benefits, if they exist at all, will be negligible, the lifting the limitation on liability will likely lead to less socially desirable outcomes.

4. Examples of Existing Limitation on Liability Provisions

Limitations on liability provisions are ubiquitous in commercial relations and in the securities and finance businesses. While the SEC-regulated relationship between the SROs and the Industry Members limit the applicability of general commercial contractual considerations to limitations on liability regarding cyber security at CAT, there are multiple examples where public (and private) interests have been served by limitations on liability provisions imposed by regulation. Some of these instances are common in the investment business while others are in areas remote from investment but exhibit informative parallels.

---

121 There is an extensive literature on the incidence of the corporate income tax supporting this proposition. In this literature, owners have a greater ability to adjust their decisions (especially how they invest their capital) than employees or customers. See, for example, William M. Gentry, "A Review of the Evidence on the Incidence of the Corporate Income Tax," *U.S. Department of the Treasury OTA Paper 101*, December 2007 (https://www.treasury.gov/resource-center/tax-policy/tax-analysis/Documents/WP-101.pdf accessed August 2020); Jennifer C. Gravelle, "Corporate Tax Incidence: A Review of Empirical Estimates and Analysis," *Congressional Budget Office Working Paper 2011-01*, June 2001 (https://www.cbo.gov/sites/default/files/cbofiles/ftpdocs/122xx/doc12239/06-14-2011-corporatetaxincidence.pdf accessed August 2020); and Stephen Entin, "Labor Bears Much of the Cost of the Corporate Tax," *Tax Foundation Special Report No. 238*, October 2017 (https://files.taxfoundation.org/20181107145034/Tax-Foundation-SR2382.pdf accessed August 2020). For a more comprehensive treatment of tax incidence, see Don Fullerton and Gilbert E. Metcalf, "Tax Incidence," Chapter 26 (pp. 1787-1872) in Alan Auerbach and Martin Feldstein, *Handbook of Public Economics*, 2002. A working paper version of this chapter can be found at https://www.nber.org/papers/w8829.pdf accessed August 2020.

We contend that this literature is applicable to adding litigation exposure from cyber breaches to CAT and the Plan Processor with minor modifications in the analysis. As noted above, litigation is an additional expense for CAT and the Plan Processor. For CAT and the Plan Processor to operate, expenses must be paid. By CAT's funding principles, the extra funds will be passed along as higher fees to the Participants and the Industry Members.

Perhaps most relevant are the limitations of liability provision imposed by existing trade reporting facilities, regulatory reporting systems, and Industry Member agreements with their customers. Here, the Industry Members routinely (and unremarkably) specifically limit their liability to their respective customers, even though Industry Members hold important and sensitive customer information in their systems. The May 6, 2020 *Consolidated Audit Trail, LLC's and Participants' Memorandum of Law in Opposition to SIFMA's Motion to Stay* documents,

> *[T]he Limitation of Liability Provision is similar in substance and scope to provisions that Industry Members routinely use when they are in possession of customer data (including order and trade data). Finally, each exchange has rules, approved by the Commission, that broadly provide that the Participants shall not be liable to Industry Members.*[122]

One finds limitations of liability elsewhere in the U.S. economy where the threat of litigation would raise costs and regulation exists. The examples presented below limit liability while simultaneously providing another mechanism to compensate injured parties.

The federal government, for example, has established a limitation of liability for vaccine producers. The National Childhood Vaccine Injury Act of 1986[123] established the National Vaccine Injury Compensation Program "after lawsuits against vaccine manufacturers and healthcare providers threatened to cause vaccine shortages and reduce vaccination rates."[124] This legislation limited the liability of vaccine manufacturers for unavoidable adverse side effects and for failure to provide direct warnings.[125] The liability limitation was intended "[t]o ensure a

---

122 *Consolidated Audit Trail, LLC's and Participants' Memorandum of Law in Opposition to SIFMA's Motion to Stay*, May 6, 2020, pp. 6-7. Also see, pp. 16-17 and *Appendix A: Limitation of Liability Provisions*. Internal references to Exhibit A containing the specific examples are omitted.

123 Public Health Service Act, January 5, 2017, As Amended Through P.L. 114-255, Enacted December 13, 2016, https://www.hrsa.gov/sites/default/files/hrsa/vaccine-compensation/about/title-xxi-phs-vaccines-1517.pdf accessed July 2020.

124 Health Resources & Services Administration, *About the National Vaccine Injury Compensation Program*, https://www.hrsa.gov/vaccine-compensation/about/index.html accessed July 2020.

125 *No vaccine manufacturer shall be liable in a civil action for damages arising from a vaccine-related injury or death associated with the administration of a vaccine after October 1, 1988, if the injury or death resulted from side effects that were unavoidable even though the vaccine was properly prepared and was accompanied by proper directions and warnings.*

No vaccine manufacturer shall be liable in a civil action for damages arising from a vaccine-related injury or death associated with the administration of a vaccine after October 1, 1988, solely due to the manufacturer's failure to provide direct warnings to the injured party (or the injured party's legal representative) of the potential dangers resulting from the administration of the vaccine manufactured by the manufacturer.

stable vaccine supply by limiting liability for vaccine manufacturers and vaccine administrators."[126]

In 2005, Congress passed the "Public Readiness and Emergency Preparedness Act" ("PREP Act").[127] This act extended targeted liability protections for pandemic and epidemic products and security countermeasures:

> *Subject to the other provisions of this section, a covered person shall be immune from suit and liability under Federal and State law with respect to all claims for loss caused by, arising out of, relating to, or resulting from the administration to or the use by an individual of a covered countermeasure if a declaration under subsection (b) has been issued with respect to such countermeasure.*[128]

In a declaration effective February 4, 2020, the Secretary of Health and Human Services "invoked the PREP Act and declared Coronavirus Disease 2019 (COVID-19) to be a public health emergency warranting liability protections for covered countermeasures."[129] There is currently substantial discussion regarding a legislative proposal to limit the liability of entities recommencing operations in the face of the COVID-19 pandemic.[130]

---

42 U.S. Code § 300aa-22, https://www.law.cornell.edu/uscode/text/42/300aa-22 accessed November 2020.

126 Health Resources & Services Administration, *The National Vaccine Injury Compensation Program (VICP)*, https://www.hrsa.gov/sites/default/files/hrsa/vaccine-compensation/vaccine-injury-infographic-2017.pdf accessed August 2020.

127 42 U.S. Code § 247d-6d at Health Resources & Services Administration, https://www.hrsa.gov/sites/default/files/gethealthcare/conditions/countermeasurescomp/covered_countermeasures_and_prep_act.pdf accessed July 2020.

128 42 U.S. Code § 247d-6d at Health Resources & Services Administration, https://www.hrsa.gov/sites/default/files/gethealthcare/conditions/countermeasurescomp/covered_countermeasures_and_prep_act.pdf accessed July 2020.

129 Congressional Research Service, *The PREP Act and COVID-19: Limiting Liability for Medical Countermeasures*, at https://crsreports.congress.gov/product/pdf/LSB/LSB10443 accessed July 2020.

130 See, for example, Andrew Duehren, "Senate GOP Aims to Funnel Covid Liability Cases to Federal Courts," *The Wall Street Journal*, July 16, 2020, https://www.wsj.com/articles/gop-senators-move-ahead-with-coronavirus-liability-plan-11594929198?mod=searchresults&page=1&pos=3 (accessed December 2020) and a version of this article on page A4 of the July 17, 2020 print.

> *The proposal, which the White House is reviewing, temporarily offers schools, businesses, health-care providers and nonprofit organizations legal protections when people allegedly exposed to the coronavirus sue them, according to a summary seen by The Wall Street Journal.*
>
> *Under the proposal, defendants in those cases would only be held liable if they didn't make reasonable efforts to comply with public-health guidelines and instead*

The parallel between the public policy for vaccines and the role of CAT LLC to improve investor protection and promote market integrity, particularly during times of market stress, while not exact, is useful. In this metaphor, cyber criminals play the role of viruses. Society has an interest to promote the development of a vaccine to combat the pandemic or to use the CAT to help regulate financial markets to promote the public good. Limiting liability is one way to do so.

There is a third, simultaneously more expansive and more focused example – financial solvency regulation. This is again ubiquitous and multifaceted – deposit insurance, pension guaranty coverage, insurance guaranty associations, etc. working across many types of financial institutions and products. These programs provide various customers and other stakeholders the ability to seek compensation for claims they have against the assets of a financial institution that is declared insolvent by the regulator overseeing the firm. Bank deposit insurance is a pre-funded plan financed through fees paid by regulated entity. State insurance guaranty funds are generally financed by *ex post* assessments required of insurers still solvent in a state after another insurer is declared insolvent by the regulator. Several other programs exist with varying details. It is possible a mechanism could be established that would create a pool of funds that could be used to compensate those who suffer losses due to a cyber breach of CAT. While developing a specific recommendation is beyond the scope of this assignment, we present several initial ideas in the next section of this White Paper.

Finally, there are risks that are just part of doing business that cannot be avoided or transferred to other parties through contract or insurance. The mere act of investing entails risk, for example, and the SEC is charged with managing and mitigating this risk for investors and the economy while simultaneously obtaining the benefits of the capital markets. Industry Members, for example, assume risks associated with transacting with their customers. While most are legal and legitimate, malicious parties do transact in the securities markets. The SEC has mandated that broker-dealers "know their customer" and although broker-dealers make extensive efforts to comply with this mandate, bad actors slip through. Industry Members also assume counterparty risk. There are mechanisms in place to mitigate and remediate this risk, but it can never be completely eliminated. There are also other legislative, regulatory, and political risks associated with the securities markets.

---

demonstrated gross negligence or intentional misconduct, according to the summary. The defendants would have the right to move the case to federal court if they so choose, offering a potentially more favorable alternative to state courts.

For coronavirus-related personal injury and medical liability cases, the plan also sets a clear-and-convincing-evidence burden of proof, places a cap on damages and heightens pleading standards. . . .

The legislation from Messrs. McConnell and Cornyn also shields employers from lawsuits arising from coronavirus testing in the workplace and from agency probes for steps they took to comply with stay-at-home orders. The Republicans also want to limit liability for new types of personal protective equipment if the equipment meets certain federal standards.

A certain level of cyber risk is already present in the normal business operations of the Industry Members. They accept (and manage) these risks in the expectation that they will obtain a profit from the activities that embed the risks. They have expressed concern over a possible expansion of those cyber risks to themselves and their clients as a result of the mandated transmission of information to the CAT. This transmission was mandated, and is governed, by the primary federal regulator of the Industry Members' activities. The CAT does not exist to serve customers and obtain a profit, but to help the SEC and the SROs in their regulation of the U.S. equity and option markets. While the Industry Members' concern over a possible increase in cyber risk exposure may be understandable in certain contexts, their position that the CAT and the Plan Processor be denied a limitation on liability essentially shifts the burden of cyber risk onto the regulators and regulatory process. As explained above, the SEC has already implemented standards, policies, and practices to mitigate cyber risk in the system as a whole.

E. Initial Thoughts on Funding Compensation Mechanisms

While we have concluded above that the regulatory approach to the CAT's cyber security is preferred over a litigation approach because overall social costs of control would be lower and there is no meaningful benefit from adding a litigation option as proposed by Industry Members, there is still a risk that Industry Members or their customers could be harmed in the case of a significant cyber breach. The current regulatory approach is generally silent on the possibility of compensating third parties in the case of a CAT cyber breach. Of concern here is the possibility of a previously unseen cyber event that results in a high damage/severity "black swan" type event.

There are, however, several approaches to designing and funding potential compensation mechanisms.

The use of cyber insurance, for example, could be advantageous. Cyber coverage can be purchased as part of a package of business insurance (property-casualty and liability) or as a stand-alone policy. According to information supplied to state regulatory authorities in the U.S., in 2019 stand-alone cyber policies exhibited somewhat higher premium receipts than cyber coverage included in broader packages – $1.26 billion and $1 billion, respectively.[131] This was an 11 percent increase from 2018, with 192 insurers reporting direct cyber written premium in 2019.[132] Between 2017 and 2019, the number of cyber claims doubled to 18,000.[133] Over the

---

131 Aon plc, *US Cyber Market Update: 2019 US Cyber Insurance Profits and Performance*, June 2020, p. 3, Exhibit 2, http://thoughtleadership.aon.com/Documents/202006-us-cyber-market-update.pdf accessed July 2020. Very similar figures were reported by A.M Best – $1.26 billion for stand-alone and $988 million for package policies. Erin Ayers, "US cyber market keeps growing, but pace slowed: AM Best," *Advisen Front Page News*, July 22, 2020 accesed August 2020.

132 Aon plc, *US Cyber Market Update: 2019 US Cyber Insurance Profits and Performance*, June 2020, p. 3, Exhibit 1, http://thoughtleadership.aon.com/Documents/202006-us-cyber-market-update.pdf accessed July 2020.

133 Erin Ayers, "US cyber market keeps growing, but pace slowed: AM Best," *Advisen Front Page News*, July 22, 2020 accessed August 2020.

2015 through 2019 period, paid losses plus defense costs ranged from just under 30% to just above 50% of premiums.[134] The reported 2019 expense ratio for cyber coverage averaged just under 30% of premiums.[135] In 2019, almost two-thirds of the cyber claims were for first-party losses with the remaining being for third-party losses.[136]

The use of cyber insurance extends the assets available to compensate injured parties and therefore mitigates some of the judgement-proof problem discussed above. While the cyber insurance market is relatively new and undeveloped compared to a number of other coverages,[137] it focuses on understanding and quantifying the frequency and severity of cyber breaches along with efforts to identify and promote methods to mitigate those risks. Reinsurance companies, in particular, "can help to develop products and share underwriting know-how, including modeling experience. . . Reinsurers can also play a role in establishing cyber ecosystems by offering holistic cyber solutions through services and relationships with cybersecurity companies, specialized managing general agents, or insurtech companies."[138] Assuming that an insurer's cyber coverage premium to the CAT and the Plan Processor is related to an informed evaluation of the risks posed, cyber premiums can provide additional incentives to the CAT and the Plan Processor to internalize the cost of its security decisions and actions.[139] If cyber insurance rates

---

134 Aon plc, *US Cyber Market Update: 2019 US Cyber Insurance Profits and Performance*, June 2020, pp. 4-5, Exhibits 3 and 4, http://thoughtleadership.aon.com/Documents/202006-us-cyber-market-update.pdf accessed July 2020.

135 Aon plc, *US Cyber Market Update: 2019 US Cyber Insurance Profits and Performance*, June 2020, p. 7, Exhibit 7, http://thoughtleadership.aon.com/Documents/202006-us-cyber-market-update.pdf accessed July 2020. The expense ratio combines the selling and underwriting costs of a coverage and divides that by the premium receipts associated with that coverage.

136 Aon plc, *US Cyber Market Update: 2019 US Cyber Insurance Profits and Performance*, June 2020, p. 9, Exhibit 10, http://thoughtleadership.aon.com/Documents/202006-us-cyber-market-update.pdf accessed July 2020. The expense ratio combines the selling and underwriting costs of a coverage and divides that by the premium receipts associated with that coverage.

137 "Insured cyber losses remain a fraction of total economic cyber losses caused by cybercrime, with about $6 billion of insured losses in total (affirmative and nonaffirmative [e.g., "silent"] cyber losses), versus $600 billion of economic losses in 2018." S&P Global Ratings, *Global Reinsurance Highlights 2019,* p. 29. See also, Sasha Romanosky, Lillian Ablon, Andreas Kuehn and Therese Jones, "Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?" *Journal of Cybersecurity*, 2019, pp. 1-19.

138 S&P Global Ratings, *Global Reinsurance Highlights 2019,* p. 31.

139 Romanosky *et al* (2019) report that while some insurers currently employ sophisticated pricing algorithms and incorporate specific security information to determine the premiums they charge for cyber insurance, at present the majority of the market uses relatively simple rate forms and generic self-assessed risk vulnerability categorizations

reflect anticipated costs of the cyber risks, and CAT LLC and FINRA CAT pay the premiums, then the CAT's costs incorporate (internalize) the expected costs of a cyber breach under the terms of the coverage.

For many insurers, cyber coverage entails a relatively high degree of monitoring of the insureds. The insurers also have on retainer cyber mitigation and remediation experts that are independent of the insureds and focused on reducing the risk of cyber incursion. A 2017 publication by the Organisation for Economic Co-operation and Development ("OECD") noted the following:

> *In addition to providing insurance coverage for the expenses incurred as a result of a cyber incident, many insurance companies provide additional services with their policies, either as risk management advice during the underwriting process, as a means to reduce vulnerability to cyber incidents during the period of coverage or in order to reduce the impact of cyber incidents that occur. The first two types of services are often referred to as pre-breach services or risk mitigation services while the latter type is identified as post-breach or response services. Some insurance companies have developed significant internal expertise and offer these types of services directly, while others have developed networks and/or partnerships with a variety of service providers, often involving some form of discounted pricing for its policyholders (e.g. information technology security consultants, legal firms, public relations firms, etc.)*
>
> *. . . [S]ome insurance companies provide specific risk assessment services as part of the underwriting process (sometimes even if no insurance coverage is entered into) ranging from online or onsite security assessments to advice on security policies and practices, to vulnerability scans and penetration testing which should benefit both the insurance company and the company's risk management (omitted internal cites). Insurance companies are also offering an assortment of risk mitigation services during the coverage period, including threat and intelligence warnings and detection, access to specialised protection technologies, preparation and testing of contingency plans, helplines or information portals and employee training (omitted internal cites).*
>
> *A range of services for managing the impact of a cyber incident are also being offered, including forensic investigative services necessary to identify the source of any breach, legal assistance to help manage legal and regulatory requirements and potential liability, providers of call centre capacity, notification services, credit monitoring and/or identity theft protection to support interaction with affected*

(e.g., low, medium, high). As recent demand growth has been high and profitability strong, we expect more insurers will continue to enter this market that will then attract additional industry vendors, capital markets risk intermediaries, risk modeling firms, reinsurers, and brokers, etc., to also enter the market. The increased competition will bring increasing levels of sophistication and with it we expect insurance premiums will become more and more risk sensitive over time. See Sasha Romanosky, Lillian Ablon, Andreas Kuehn and Therese Jones, "Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?" *Journal of Cybersecurity*, 2019, pp. 1-19.

clients, and public relations companies to minimise the reputational impact of cyber incidents (omitted internal cites).

According to one survey, 70% of insurers provide (or plan to provide) cyber risk mitigation or response services . . . . Seventeen of the 23 policies reviewed by the OECD advertised access to risk mitigation and/or response services. . . .[140]

A manuscripted (i.e., customized), stand-alone cyber insurance policy for CAT could be combined with other approaches. If the SEC were to approve such an arrangement, the CAT and/or the Plan Processor could issue insurance linked securities, such as industry loss warranties or catastrophe bonds that could attract capital market investors to underwrite the losses in addition to insurers and reinsurers. Industry loss warranties are insurance or reinsurance contracts in which coverage is triggered by an industry-wide loss or by an index exceeding some pre-specified amount. Catastrophe bonds are fixed income instruments where the "debtor" (the CAT or the Plan Processor) pays "interest" (similar to premiums) to the "creditor" (the "insurer" or the "capital market investor"), who does not lend the money but promises to pay the funds should a specified cyber event happen.[141]

At present, we are aware of a few cyber-related industry loss warranties that have been issued.[142] No cyber catastrophe bond has yet been issued, but industry observers suggest now may be the time to see such an advance. Commenting on the state of the cyber insurance market, the enormous potential size of the economic losses due to cyber events, and the recent growth of cyber-related insurance premiums, Standard & Poor's believes it is only a matter of time before industry capacity will be insufficient alone to satisfy demand and that governments and capital markets will come together with the industry to create markets that can meet the capacity requirements for cyber coverage.[143]

---

140 Organisation for Economic Co-operation and Development, *Enhancing the Role of Insurance in Cyber Risk Management*, (2017), Chapter 3, "The cyber insurance market," pp. 75-76, https://www.oecd-ilibrary.org/docserver/9789264282148-5-en.pdf?expires=1595620895&id=id&accname=guest&checksum=84A71DC31B31AD5ADA3B29E4BCA3BD62 accessed July 2020.

141 "The Singaporean government's plans to introduce a commercial cyber pool with re/insurers and insurance-linked security (ILS) backing capacity is a recent example. However, before ILS investors will accept cyber risk as a potential investment opportunity, the market will need to enhance its ability to model this risk as well as have a longer track record." S&P Global Ratings, *Global Reinsurance Highlights 2019*, p. 31.

142 Shah, Syed Salman, and Ben Dyson, "Cyber insurance-linked securities have arrived, but market still in infancy," *S&P Global Market Intelligence,* https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/cyber-insurance-linked-securities-have-arrived-but-market-still-in-infancy-46915334 accessed September 2020.

143 Bender, Johannes, Manuel Adam, Robert J Greensted, Jean Paul Huby Klein, Milan Kakkad, and Tracy Dolin, "Global Reinsurers Face the Iceberg Threat Of Cyber Risk," *Global Reinsurance Highlights 2019* (2019) pp. 28-31.

We mentioned earlier in the White Paper that several funding mechanisms exist to compensate the customers of financial intermediaries, subject to limits, including banks, credit unions, and insurance companies. Under the auspices of the SEC, one could also imagine self-funding a third-party compensation program. Some combination of any of these approaches, and others, might be considered. The goal here is to mitigate the damages of a cyber breach and compensate affected third parties in the lowest cost fashion. Industry Members should recognize that, ultimately, it is they, the SROs, and especially their customers that will pay all the costs of the CAT.

IV. Conclusion

This White Paper investigates the SEC's regulatory approach to the CAT's cyber security and conducts an economic analysis to examine whether adding an ability for Industry Members to litigate in the event of a CAT cyber breach creates socially optimal incentives for controlling the cyber risk exposures faced by CAT over a regulation alone approach.

As explained in this White Paper, the economic role of litigation is to provide meaningful *ex-ante* incentives for first parties to internalize the harms potentially caused to third parties by their economic activities through the threat they may face *ex post* litigation filed by the injured third parties. Regulation, however, also provides meaningful incentives for first parties to internalize the harms they may potentially cause to third parties by compelling first parties to follow a set of rules and procedures proscribed by a regulator before the economic activity commences.

An economic analysis of the circumstances attending the CAT shows that regulation by the SEC already properly incentivizes the Participants to recognize and address the risks that a CAT cyber breach poses to third parties such as Industry Members. We further show that the possibility of permitting litigation by Industry Members in addition to the regulatory regime will not meaningfully increase CAT's incentives to manage its exposure to cyber risk, yet it will significantly increase the costs (which will ultimately be passed on to retail investors) that it bears to do so. Our analysis suggests that the *ex-ante* regulation approach *alone* leads to the socially optimal outcome.

Accordingly, our analysis of the respective benefits of *ex-ante regulation* compared with *ex post litigation* indicate that the limitation of liability in the proposed CAT Reporter Agreement will serve the public interest.

The authors of this paper are employed by, or affiliated with, Charles River Associates (CRA). The conclusions set forth herein are based on independent research and publicly available material. The views expressed herein are the views and opinions of the authors only and do not reflect or represent the views of Charles River Associates or any of the organizations with which the authors are affiliated. Any opinion expressed herein shall not amount to any form of guarantee that the authors or Charles River Associates has determined or predicted future events or circumstances and no such reliance may be inferred or implied. The authors and Charles River Associates accept no duty of care or liability of any kind whatsoever to any party, and no responsibility for damages, if any, suffered by any party as a result of decisions made, or not made, or actions taken, or not taken, based on this paper. Detailed information about Charles River Associates, a registered tradename of CRA International, Inc., is available at www.crai.com.

V. Qualifications of Authors / Investigators

Michael G. Mayer, CFA, CFE **Vice President, Charles River Associates**	M.B.A. Finance and Management Policy, Kellogg Graduate School of Management, Northwestern University B.S. Marketing and Management Policy, Indiana University School of Business

Michael G. Mayer is a Vice President of Charles River Associates. He has performed numerous business valuation assignments and has evaluated numerous claims for economic loss in a range of business, banking, securities, derivatives and insurance disputes. He has also performed financial investigations of brokerage firms, hedge funds, savings & loans, banks, and insurance companies as well as in whistleblower, insider trading, and FCPA matters. He has testified as an expert in International Arbitration forums, US Federal and State Courts, AAA and FINRA arbitrations, and the Bahamian Supreme Court. Mr. Mayer's testimony has addressed financial and economic issues including investment suitability and trading, portfolio management, valuation, lost profits, loss of principal and prejudgment interest.

In litigation matters, Mr. Mayer has been most actively involved in the determination of damages in securities fraud and breach of fiduciary duty cases, broker/dealer litigation, failed mergers/acquisitions, bankruptcy, lender liability, and shareholder disputes. He is regularly called upon to analyze complex securities and explain their structures. Additionally, he has significant experience in other areas of commercial litigation including antitrust, accountant's liability, breach of contract, business interruption, and insurance. He has assisted counsel with respect to discovery and document management, deposition and cross-examination assistance and trial exhibit preparation.

Outside of litigation, Mr. Mayer regularly consults on financial issues relating to mergers, acquisitions, joint ventures, and licensing. He has analyzed and negotiated deal structures on behalf of clients in a broad range of industries ranging from pharmaceuticals to industrial rubber products. Additionally, he has performed business and intangible asset valuations for some of the largest companies in the country. Mr. Mayer has been widely quoted in the press including the Wall Street Journal, CFO Magazine, Inside Counsel Magazine, Securities Law360, and the Chicago Tribune, among others.

Mark F. Meyer **Vice President, Charles River Associates**	PhD, Economics University of Michigan BSFS, International Economics Georgetown University

Dr. Mark F. Meyer is a vice president and the co-leader of the Insurance Economics Practice of CRA. He has over 30 years of experience applying economic theory and quantitative methods to a range of complex business litigation and regulatory matters. Dr. Meyer's experience includes assessing liability and damages for litigations involving firms engaged in financial markets, especially insurance; investigations of insurer insolvencies; antitrust analysis of monopolization, mergers, and price discrimination in a wide range of industries; work in the economics of product distribution and marketing; analysis of regulatory initiatives involving insurance and other industries; and statistical and econometric applications to liability determination, market definition, class certification, and economic damages.

Prior to joining CRA, Dr. Meyer was a senior economist at the Princeton Economics Group, Inc.; senior managing economist and a director in the New York office of the Law & Economics Consulting Group, Inc.; and an economist at the law firm of Skadden, Arps, Slate, Meagher & Flom in New York.

Prof. Richard D. Phillips **Senior Consultant to Charles River Associates** **Dean, J. Mack Robinson College of Business** **C.V. Starr Professor of Risk Management and Insurance** **Georgia State University**	PhD, Insurance and Finance University of Pennsylvania MA, Insurance and Finance University of Pennsylvania BS, Mathematics University of Minnesota

Richard D. Phillips is the dean of the J. Mack Robinson College of Business, Georgia State University, and the C.V. Starr Professor of Risk Management and Insurance. He has served as a Senior Consultant to CRA since 2010.

Dr. Phillips was the associate dean for academic initiatives and innovations from 2012 until 2014 and from 2006 to 2012 he was the Kenneth Black Jr. Chair of the Department of Risk Management and Insurance. From 1997 until 2014 he held the appointment of Fellow of the Wharton Financial Institutions Center at the University of Pennsylvania. He has held visiting appointments at the Federal Reserve Bank of Atlanta (1996–1997), at the Wharton School (2003), at the Federal Reserve Bank of New York (2007–2008), and he was the Swiss Re Visiting Scholar at the University of Munich in 2008. Dr. Phillips joined Georgia State University after completing his doctoral studies at the University of Pennsylvania in 1994.

Professor Phillips' research interests lie at the intersection of corporate finance and insurance economics with specific focus on the effect of risk on corporate decision-making, and the functioning of insurance markets. He has published in academic and policy journals including the *Journal of Financial Economics,* the *Journal of Risk and Insurance,* the *Journal of Banking and Finance, Journal of Financial Services Research,* the *Journal of Law and Economics,* the *Journal of Insurance Regulation,* and the *North American Actuarial Journal*, among others. He has contributed scholarly articles to books published by Risk Publications, the University of Chicago Press, Kluwer Academic Publishers, and the Brookings Institute. Professor Phillips has received several awards for his research including the Robert I. Mehr Research Award (2008, 2009), the Robert C. Witt Research Award (1999), the ARIA/CAS Best Paper Award three times (1998, 1999, and 2006), and the James S. Kemper Best Paper Award (2003) among others. He served on the board of directors and is a Past President of the American Risk and Insurance Association, he is a Past President of the Risk Theory Society and is a Past Co-editor of the *Journal of Risk and Insurance.* He serves as an *ad hoc* referee for several academic journals.

Beyond the university, Professor Phillips has served as a consultant to numerous commercial and governmental organizations throughout his career including AIG, Allstate, ING, AXA, Deutsche Bank, Goldman Sachs, Tillinghast, Aon Capital Markets, the Casualty Actuarial Society, the Society of Actuaries, and the U.S. Office of Management and Budget. He is a member of the board of directors for the Munich American Reassurance Company. Within the non-profit sector, Professor Phillips was the Executive Director of Georgia State University's Risk Management Foundation from 2006–2012, he is a board member on the S.S. Huebner Foundation for Insurance Education Foundation, he is a board member of the World Affairs Council of Atlanta, and he is Chairman Emeritus of the Board of Trustees for the Swift School, one of the largest private-independent schools serving dyslexic students grades 1-8 in Georgia.

Rona T. Seams **Principal, Charles River Associates**	M.B.A. Finance, Management and Strategy, Marketing, Kellogg Graduate School of Management, Northwestern University B.B.A. Finance, University of Texas-Austin

Ms. Seams is a Principal at CRA and has testified as an economic damages expert in federal court and has been involved in and managed numerous other engagements involving financial investigations, economic damages, and business valuations.

Ms. Seams has performed financial investigation activities in many matters including the alleged mismanagement of bank investments by its management, the alleged breach of fiduciary duty of FNMA for not detecting fraud perpetrated on an entity selling mortgages to FNMA, the alleged acquisition of life settlement policies through bid rigging, and the alleged profit made by trading on inside information.

Ms. Seams' economic damages work includes the determination of damages related to the breach of a non-compete agreement in the equipment leasing industry, the assessment of damages related to the raiding of employees in the securities industry, the calculation of damages related to fraud perpetrated on a temporary staffing company, the damages analysis for the creditors of a large bankrupt energy trading company, the valuation of damages associated with securities fraud, the determination of early contract termination damages in the securities clearing industry, and the calculation of intellectual property damages across many industries.

Ms. Seams' business valuation work includes the net worth analysis of a company to pay an award of punitive damages, the solvency analysis of a regional acute care hospital, the solvency analysis of a temporary staffing company, and the valuation of an energy storage and distribution company.

Prior to joining Charles River Associates, Ms. Seams operated her own consulting firm specializing in project finance, contract analysis, and sales and risk management. Additionally, she worked in the energy industry in various roles ranging from rate analyst, market analyst, sales representative, and management consultant.

VI. Research Program and Bibliography

The authors of this White Paper have thoroughly reviewed extensive publicly available documents and obtained information from CAT LLC and FINRA CAT personnel to understand the circumstances surrounding the CAT and develop their findings. We also rely on longstanding bodies of economic literature regarding cyber breaches and creating socially optimal incentives to control risk (including risk of cyber breaches). The following documents in the Securities and Exchange Commission record for the Consolidated Audit Trail, which we reviewed closely, were particularly informative on CAT LLC and the considerations and concerns of various interested parties.

- Securities and Exchange Commission, *Consolidated Audit Trail*, Release No. 34-67457.
- Securities and Exchange Commission, *Joint Industry Plan; Order Approving the National Market System Plan Governing the Consolidated Audit Trail,* Release No. 34-79318, November 15, 2016. Attachments to this document included:
    - The March 3, 2014 CAT NMS Plan Request for Proposal,
    - The Limited Liability Company Agreement of CAT LLC,
    - The Participants' Discussion of Considerations, and
    - The CAT NMS Plan Processor Requirements.
- Securities and Exchange Commission, *Order Granting Conditional Exemptive Relief, Pursuant to Section 36 and Rule 608(e) of the Securities Exchange Act of 1934, from Section 6.4(d)(ii)(C) and Appendix D Sections 4.1.6, 6.2, 8.1.1, 8.2, 9.1, 9.2, 9.4, 10.1, and 10.3 of the National Market System Plan Governing the Consolidated Audit Trail,* Release No. 34-88393, March 17, 2020.
- Securities and Exchange Commission, *Amendments to the National Market System Plan Governing the Consolidated Audit Trail*, RIN 3235-AM60, Release No. 34-88890, File No. S7-13-19, May 15, 2020.
- Securities and Exchange Commission, *Amendments to the National Market System Plan Governing the Consolidated Audit Trail to Enhance Data Security*, RIN 3235-AM62, Release No. 34-89632, File No. S7-10-20, August 21, 2020.
- *Memorandum of Law in Support of SIFMA's Motion to Stay SRO Action Pending Commission Review of SIFMA's Application Pursuant to Exchange Act Sections 19(d) and 19(f),* April 22, 2020.

In addition to the documents listed above, the authors investigated the implementation of cyber security at the CAT by thoroughly reviewing the extensive document record listed below and by obtaining information from personnel at FINRA CAT responsible for compliance and cyber security.

- Consolidated Audit Trail, LLC and FINRA CAT, LLC, *Industry Webinar – Security of CAT Data*, April 1, 2020, at https://www.catnmsplan.com/events/industry-webinar-security-cat-data-412020, accessed September 2020.

- Amazon Web Services website, "Cloud computing with AWS," at https://aws.amazon.com/what-is-aws/?sc_icampaign=aware_what_is_aws&sc_icontent=awssm-evergreen-prospects&sc_iplace=hero&trk=ha_awssm-evergreen-prospects&sc_ichannel=ha, visited September 2020.

- Amazon Web Services website, "Cloud computing with AWS, Most secure" at https://aws.amazon.com/what-is-aws/?sc_icampaign=aware_what_is_aws&sc_icontent=awssm-evergreen-prospects&sc_iplace=hero&trk=ha_awssm-evergreen-prospects&sc_ichannel=ha, visited September 2020.

The other sources the authors relied upon to form their opinions are:

Cyber Security Risk Analysis:

1. Advisen Cyber OverVue, https://insite20twenty.advisen.com.
2. Advisen's Cyber OverVue User Guide, January 2020.
3. Advisen, *Quarterly Cyber Risk Trends: Global Fraud is Still on the Rise*, sponsored by CyberScout, Q2 2019.
4. Advisen website, https://www.advisenltd.com/data/cyber-loss-data/.
5. Advisen website, www.advisenltd.com.
6. AllAboutAlpha, "High-Frequency-Trading Firms: Fast, Faster, Fastest," April 2, 2019, https://www.allaboutalpha.com/blog/2019/04/02/high-frequency-trading-firms-fast-faster-fastest/.
7. Alexander Osipovich, "High Speed Trader Virtu Discloses $6.9 Million Hacking Loss," *Dow Jones News Service*, August 11, 2020.
8. Allied Market Research website, *Cyber Insurance Market by Company Size and Industry Vertical: Global Opportunity Analysis and Industry Forecast, 2019-2026*, March 2020, https://www.alliedmarketresearch.com/cyber-insurance-market.
9. Camico website, "Understanding First-Party and Third-Party Cyber Exposures," https://www.camico.com/blog/understanding-cyber-exposures.
10. Capital IQ Website, https://www.capitaliq.com/CIQDotNet/Financial/Capitalization.aspx?CompanyId=133624510.
11. *CAT Reporting Technical Specifications for Industry Members*, Version 3.1.0 r2, April 21, 2020.

12. The Center for Strategic and International Studies, "Net Losses: Estimating the Global Cost of Cybercrime," June 2014.

13. Chairman Jay Clayton, Testimony on "Oversight of the Securities and Exchange Commission" Before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, December 10, 2019, https://www.sec.gov/news/testimony/testimony-clayton-2019-12-10.

14. Commissioner Luis A. Aguilar, U.S. Securities and Exchange Commission, "The Need for Robust SEC Oversight of SROs," May 8, 2013, https://www.sec.gov/news/public-statement/2013-spch050813laahtm.

15. Commissioner Pierce Statement on Proposed Amendments to the National Market System Plan Governing the Consolidated Audit Trail to Enhance Data Security, Aug. 21, 2020, https://www.sec.gov/news/public-statement/peirce-nms-cat-2020-08-21.

16. The Council of Economic Advisers, "The Cost of Malicious Cyber Activity to the U.S. Economy," February 2018, https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

17. Cybersecurity Ventures, "Global Cybercrime Damages Predicted to Reach $6 Trillion Annually By 2021," Copyright 2020, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

18. Cyentia Institute, *Information Risk Insights Study, A Clearer Vision for Assessing the Risk of Cyber Incidents*, 2020.

19. Department of Homeland Security, "Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar," 2019, https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf.

20. Erin Ayers, "US cyber market keeps growing, but pace slowed: AM Best," Advisen Front Page News, July 22, 2020.

21. Final Judgement as to Defendant CR Intrinsic Investors, LLC, United States District Court, Southern District of New York, 12 Civ. 8466 (VM), filed June 18, 2014.

22. FINRA Investor Education Foundation, "Investors in the United States, A Report of the National Financial Capability Study" December 2019.

23. Fintel website, Berkshire Hathaway Inc – Warren Buffett – Activist 13D/13G Filings, https://fintel.io/i13d/berkshire-hathaway.

24. Gregory Meyer, Nicole Bullock and Joe Rennison, "How high-frequency trading hit a speed bump," *Financial Times*, January 1, 2018, https://www.ft.com/content/d81f96ea-d43c-11e7-a303-9060cb1e5f44.

25. Interview with William Hardin, VP, Charles River Associates, August 11, 2020.

26. Investopedia website, Toehold Purchase definition, https://www.investopedia.com/terms/t/toeholdpurchase.asp.

27. Jane Croft, "Citadel Securities sues rival over alleged trading strategy leak," *Financial Times,* January 10, 2020, https://www.ft.com/content/2cbf1738-33cd-11ea-9703-eea0cae3f0de.

28. Jensen and Ruback, "The Market for Corporate Control," *Journal of Financial Economics,* 11, (1983).

29. Journal of Forensic & Investigative Accounting, "Market Efficiency and Investor Reactions to SEC Fraud Investigations," Vol. 2, Issue 3, Special Issue, 2010.

30. Julian Hayes, "Double extortion: An emerging trend in ransomware attacks," *Advisen Front Page News,* August 21, 2020, https://www.advisen.com/tools/fpnproc/fpns/articles_new_35/P/375350842.html?rid=375350842&list_id=35.

31. Juniper Research, "Business Losses to Cybercrime Data Breaches to Exceed $5 Trillion By 2024," August 27, 2019, https://www.juniperresearch.com/press/press-releases/business-losses-cybercrime-data-breaches.

32. Memorandum from SEC Division of Trading and Markets to SEC Market Structure Advisory Committee dated October 20, 2015 with the subject "Current Regulatory Model for Trading Venues and for Market Data Dissemination," https://www.sec.gov/spotlight/emsac/memo-regulatory-model-for-trading-venues.pdf.

33. Nathan Vardi, "Finance Billionaire Ken Griffin's Citadel Securities Trading Firm Is On A Silicon Valley Hiring Binge," *Forbes,* June 3, 2019, https://www.forbes.com/sites/nathanvardi/2019/06/03/finance-billionaire-ken-griffins-citadel-securities-trading-firm-is-on-a-silicon-valley-hiring-binge/#34f23c9c6b36.

34. NPR website, Barbara Campbell, "SEC Says Cybercriminals Hacked Its Files, May Have Used Secret Data for Trading," September 20, 2017, https://www.npr.org/sections/thetwo-way/2017/09/20/552500948/sec-says-cybercriminals-hacked-its-files-may-have-used-secret-data-for-trading.

35. Opinion and Order, SEC v. Raj Rajaratnam, et. al., United States District Court, Southern District of New York, 09 Civ. 8811 (JSR), filed November 8, 2011.

36. Ponemon Institute and IBM Security, *Cost of a Data Breach Report 2020*.

37. Refinitiv website, https://www.refinitiv.com/en/about-us.

38. Research and Markets, *Algorithmic Trading Market by Trading Type, Component, Deployment Mode, Enterprise Size, and Region – Global Forecast to 2024*, https://www.researchandmarkets.com/reports/4770543/algorithmic-trading-market-by-trading-type#rela0-4833448.

39. Research and Markets, *Algorithmic Trading market – Growth, Trends, and Forecast (2020-2025),* https://www.researchandmarkets.com/reports/4833448/algorithmic-trading-market-growth-trends-and#rela4-5125563.

40. ScienceDirect website, "Hacktivists," https://www.sciencedirect.com/topics/computer-science/hacktivists.

41. SEC's Edgar website, Berkshire Hathaway Inc filings, https://www.sec.gov/Archives/edgar/data/1067983/000095012316022377/0000950123-16-022377-index.htm.

42. SEC's Edgar website, Berkshire Hathaway Inc filings, https://www.sec.gov/Archives/edgar/data/1067983/000095012316022377/xslForm13F_X01/primary_doc.xml.

43. SEC's Edgar website, Berkshire Hathaway Inc filings, https://www.sec.gov/Archives/edgar/data/1067983/000095012316022377/xslForm13F_X01/form13fInfoTable.xml.

44. SEC website, https://www.sec.gov/forms.

45. SEC website, "SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases," Press Release 2015-163, August 11, 2015, https://www.sec.gov/news/pressrelease/2015-163.html.

46. SEC website, "SEC Reaches Settlements with Traders in Newswire Hacking and Trading Scheme," Litigation Release No. 24833, June 10, 2020, https://www.sec.gov/litigation/litreleases/2020/lr24833.htm.

47. SEC website, "Rule 613 (Consolidated Audit Trail)," https://www.sec.gov/divisions/marketreg/rule613-info.htm.

48. Teresa Suarez, "A Crash Course on Capturing Loss Magnitude with the FAIR Model," *Fair Institute website*, October 20, 2017, https://www.fairinstitute.org/blog/a-crash-course-on-capturing-loss-magnitude-with-the-fair-model.

49. Terrence Hendershott, Charles M. Jones, and Albert J. Menkveld, Does Algorithmic Trading Improve Liquidity?, *The Journal of Finance*, Volume 66, No. 1, February 2011, http://faculty.haas.berkeley.edu/hender/Algo.pdf.

50. United States Census Bureau website, the U.S. and World Population Clock, https://www.census.gov/popclock/.

51. Verizon, *2020 Data Breach Investigations Report*.

52. Wharton University of Pennsylvania, "How Undisclosed SEC Investigations Lead to Insider Trading," March 2, 2020, https://knowledge.wharton.upenn.edu/article/undisclosed-sec-investigations-lead-insider-trading/.

Economic and Public Policy Analysis of Cyber Security for CAT LLC:

1. 42 U.S. Code § 247d-6d at Health Resources & Services Administration, https://www.hrsa.gov/sites/default/files/gethealthcare/conditions/countermeasurescomp/covered_countermeasures_and_prep_act.pdf.

2. 42 U.S. Code § 300aa-22, https://www.law.cornell.edu/uscode/text/42/300aa-22.

3. Andrew Duehren, "Senate GOP Aims to Funnel Covid Liability Cases to Federal Courts," *The Wall Street Journal*, July 16, 2020, https://www.wsj.com/articles/gop-senators-move-ahead-with-coronavirus-liability-plan-11594929198?mod=searchresults&page=1&pos=3.

4. Aon plc, *US Cyber Market Update: 2019 US Cyber Insurance Profits and Performance*, June 2020, http://thoughtleadership.aon.com/Documents/202006-us-cyber-market-update.pdf.
5. Bhole, Bharat, and Jeffrey Wagner, "The Joint Use of Regulation and Strict Liability with Multidimensional Care and Uncertain Conviction," *International Review of Law and Economics* Vol. 28 (2008).
6. Congressional Research Service, *The PREP Act and COVID-19: Limiting Liability for Medical Countermeasures*, https://crsreports.congress.gov/product/pdf/LSB/LSB10443.
7. *Consolidated Audit Trail, LLC's and Participants Memorandum of Law in Opposition to SIFMA's Motion to Stay*, May 6, 2020.
8. Consolidated Audit Trail website, FAQs, https://www.catnmsplan.com/faq.
9. Consolidated Audit Trail website, Security: FAQs, https://www.catnmsplan.com/faq.
10. De Geest, Gerrit, Giusseppe Dari-Mattiacci, "Soft Regulators, Tough Judges," *Supreme Court Economic Review*, Vol. 15 (2007).
11. Don Fullerton and Gilbert E. Metcalf, "Tax Incidence," Chapter 26 in Alan Auerbach and Martin Feldstein, *Handbook of Public Economics*, 2002. https://www.nber.org/papers/w8829.pdf.
12. Erin Ayers, "US cyber market keeps growing, but pace slowed: AM Best," *Advisen Front Page News*, July 22, 2020.
13. Harold Demsetz, "When Does the Rule of Liability Matter?" *Journal of Legal Studies,* Vol. 1, No. 1, (January 1972).
14. Health Resources & Services Administration, *About the National Vaccine Injury Compensation Program,* https://www.hrsa.gov/vaccine-compensation/about/index.html.
15. Health Resources & Services Administration, *The National Vaccine Injury Compensation Program (VICP)*, https://www.hrsa.gov/sites/default/files/hrsa/vaccine-compensation/vaccine-injury-infographic-2017.pdf.
16. Jennifer C. Gravelle, "Corporate Tax Incidence: A Review of Empirical Estimates and Analysis," *Congressional Budget Office Working Paper 2011-01*, June 2001. https://www.cbo.gov/sites/default/files/cbofiles/ftpdocs/122xx/doc12239/06-14-2011-corporatetaxincidence.pdf.
17. Jensen, Michael, "Agency Costs of Free Cash Flow, Corporate Finance, and Takeovers," *American Economic Review*, Vol. 76, No. 2 (May 1986).
18. Kolstad, Charles D., Thomas S. Ulen, and Gary V. Johnson, "Ex Post Liability for Harm vs. Ex Ante Safety Regulation: Substitutes or Complements?" *The American Economic Review* Vol. 80, No. 4 (Sep. 1990).
19. Mello, Michelle M., Amitabh Chandra, Atul A. Gawande, and David M. Studdert, "National Costs of the Medical Liability System," *Health Affairs*, Vol. 8, No. 9 (Sep. 2010).

20. Organisation for Economic Co-operation and Development, *Enhancing the Role of Insurance in Cyber Risk Management*, (2017), https://www.oecd-ilibrary.org/docserver/9789264282148-5-en.pdf?expires=1595620895&id=id&accname=guest&checksum=84A71DC31B31AD5ADA3B29E4BCA3BD62.

21. Public Health Service Act, January 5, 2017, As Amended Through P.L. 114-255, Enacted December 13, 2016, https://www.hrsa.gov/sites/default/files/hrsa/vaccine-compensation/about/title-xxi-phs-vaccines-1517.pdf.

22. Ronald H. Coase, "The Problem of Social Cost," *Journal of Law and Economics*, Vol 3 (1960).

23. S&P Global Ratings, *Global Reinsurance Highlights 2019.*

24. Sasha Romanosky, Lillian Ablon, Andreas Kuehn and Therese Jones, "Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?" *Journal of Cybersecurity*, 2019.

25. SEC Office of Compliance Inspections and Examinations, *Cybersecurity: Ransomware Alert*, July 10, 2020, https://www.sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf.

26. SEC website, "About the Office of Compliance Inspections and Examinations," https://www.sec.gov/ocie/Article/ocie-about.html.

27. SEC website, "Spotlight on Cybersecurity, the SEC and You," https://www.sec.gov/spotlight/cybersecurity.

28. SEC website, "Spotlight on Regulation SCI," https://www.sec.gov/spotlight/regulation-sci.shtml.

29. Shah, Syed Salman, and Ben Dyson, "Cyber insurance-linked securities have arrived, but market still in its infancy," *S&P Global Market Intelligence*, https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/cyber-insurance-linked-securities-have-arrived-but-market-still-in-infancy-46915334.

30. SIFMA website, About. https://www.sifma.org/about/.

31. Stephen Entin, "Labor Bears Much of the Cost of the Corporate Tax," *Tax Foundation Special Report No. 238*, October 2017. https://files.taxfoundation.org/20181107145034/Tax-Foundation-SR2382.pdf.

32. Steven Shavell, "Liability for Accidents," Chapter 2 in *Handbook of Law and Economics, Vol. 1*, Mitchell Polinsky and Steven Shavell, eds., Elsevier, 2007.

33. Steven Shavell, "Liability for Harm Versus Regulation of Safety," *The Journal of Legal Studies*, Vol. 13, No.2 (June 1984).

34. Steven Shavell, "The Judgement Proof Problem," *International Review of Law and Economics* Vol. 6, No. 1 (June 1 1986).

35. U.S. Court of Appeals, 2nd Circuit, Standard Investment Chartered, Inc. v. National Association of Securities Dealers, et al, https://caselaw.findlaw.com/us-2nd-circuit/1556297.html.

36. William M. Gentry, “A Review of the Evidence on the Incidence of the Corporate Income Tax,” *U.S. Department of the Treasury OTA Paper 101*, December 2007, https://www.treasury.gov/resource-center/tax-policy/tax-analysis/Documents/WP-101.pdf.