212° DATA BOILER TECHNOLOGIES, LLC

BIG DATA | BIG PICTURE | BIG OPPORTUNITIES

We see big to continuously boil down the essential improvements until you achieve sustainable growth!

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

May 3, 2021

Via Electronic Mail (rule-comments@sec.gov)

Ms. Vanessa Countryman, Secretary
U.S. Securities and Exchange Commission
100 F Street NE., Washington, DC 20549

File #	Release #	Proposed Amendments to the National Market System (NMS) Plan Governing the Consolidated Audit Trail (CAT)
4-698	34-91487 [1]	Limitation of Liability [pertaining to potential breach of privacy/ security protection of non-public data and personal identifiable information (PII)] for Stakeholders of CAT
	34-91555 [2]	Revise funding model set forth in Article XI of the CAT NMS Plan
S7-10-20	34-89632 [3]	Enhanced Data Security of CAT (RIN: 3235-AM62)

Dear Ms. Countryman:

On behalf of Data Boiler Technologies, I am pleased to provide the U.S. Securities and Exchange Commission (SEC) with our comments on the captioned releases concerning: (1) Limitation of Liability (pertaining to potential breach of privacy/ security protection of non-public data and personal identifiable information (PII) for Stakeholders of CAT system; (2) Revise funding model set forth in Article XI of the CAT NMS Plan; (3) Enhanced Data Security of CAT.

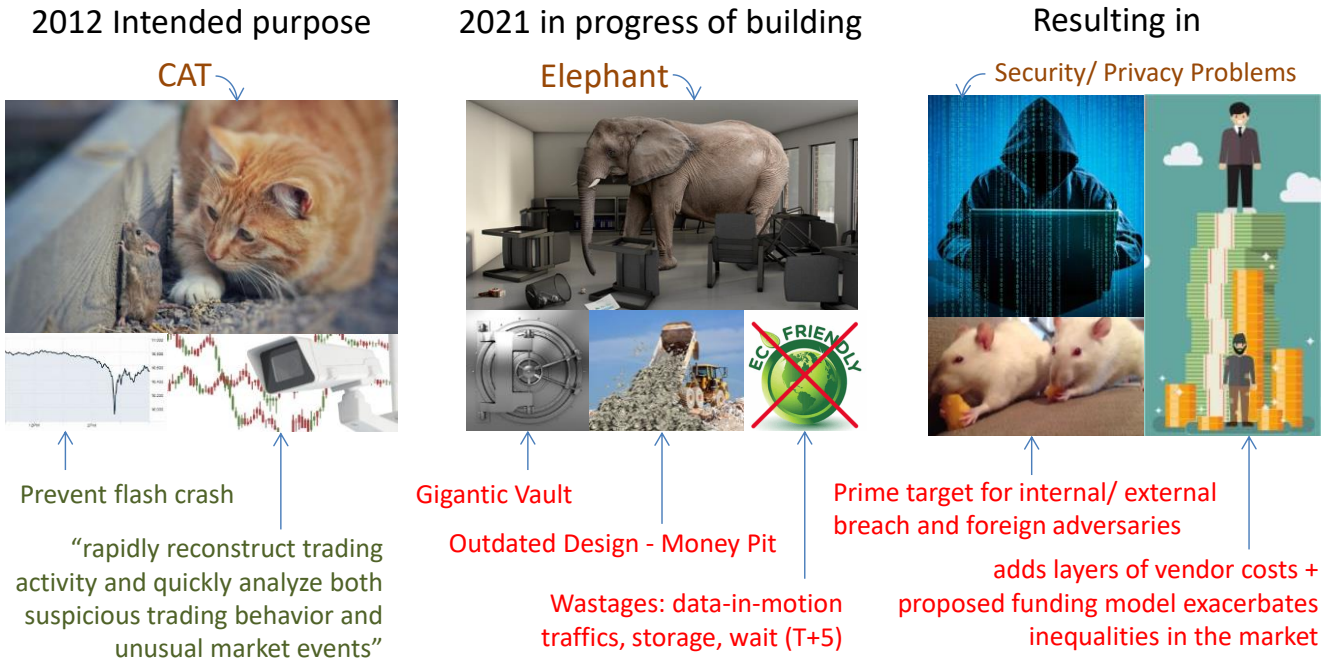
A. Context of the Problem: Outdated Design since 2012

As an inventor of patented solutions that solved the surveillance challenges mentioned in IOSCO – CR12/2012[4], we praise the honorable goals of CAT as a means to prevent future flash crashes[5] and allow the SEC and other market regulators to "rapidly reconstruct trading activity and quickly analyze both suspicious trading behavior and unusual market events"[6]. We argue **against the limitation of liability proposal and the revised funding model** NOT BECAUSE we have any dislike the CAT processor and participants (i.e. FINRA, CAT LLC, and the Exchange Groups). Indeed, **have mercy on them because every constituent** (including industry members) **seems individually bound** to achieve the following goals concurrently: (1) fulfill the SEC's mandate to regulate/ promote the safety and soundness of market, (2) the public interest [address the **civic concerns** about **Massive Government Surveillance**][7], (3) uphold and the continue pursuant of National cybersecurity and privacy protection best practices,[8] and (4) comply with the **Fourth Amendment of US Constitution**[9], the Department of Justice's latest edition of the **Privacy Act of 1974**[10] and other applicable laws and new bills[11] introduced recently.

[1] https://www.sec.gov/rules/sro/nms/2021/34-91487.pdf
[2] https://www.sec.gov/rules/sro/nms/2021/34-91555.pdf
[3] https://www.sec.gov/rules/proposed/2020/34-89632.pdf
[4] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD389.pdf
[5] https://youtu.be/dIq16lZBnDY
[6] https://www.sec.gov/news/press/2010/2010-86.htm
[7] https://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/ethics.html
[8] NIST's CISP revision 4 of SP800-53 has been superseded by revision 5 since September 2020. Also, NIST's recommended best practices alongside other Cybersecurity and Privacy protection standards/ guidelines, such as ISO/IEC 27001 and 27032, Gramm-Leach-Bliley Act §6801, and FINRA's cybersecurity rules and guidance, etc. may continue to have updates and new added contents. We have multiple concerns if CISP is referencing to a particular NIST publication, including: (1) potential of complying with the bear minimal requirements rather than pursuing the best practices; (2) new emerging cyber/ A.I. threats that the corresponding mitigation method(s) have yet to be incorporated in newer standard – i.e. the in-between time awaiting to adopt new policy; (3) non-synchronize with international rules, such as the EU's General Data Protection Regulation (GDPR).

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

The **CAT's technical design** since 2012[12] as a golden-source while well intended (or a "gigantic data-vault") **is out-of-date**. It will take "forever" to come up with a "golden" unified "single source of truth". By the time a common standard is adhered, value of the data subsided to almost worthless in the context of market surveillance. Analysts need sensors, not an encyclopedia. A good decision, made now and pursued aggressively, is substantially superior to a perfect decision made too late. The CAT project is outsized and is a **Money Pit**. Not only in terms of building and on-going operating costs, but it also introduces huge **wastages and is non-environmental friendly according to LEAN Six-Sigma**[13].



In particular, frequent transmittal of data in-and-out and within CAT, **unnecessary data-in-motion**[14] **traffics**, is wastage and more **susceptible to defects**. When data is 'at-rest' rather than 'in-use', it serves no value other than one has to pay for storage of the data. As data is **redundantly stored** at industry members' systems and at the CAT system and then is regurgitated in bulk to CAT participants' systems, causing significant **wastages**. Real-time analytic platform (RTAP) and modern techniques could be applied closest to the original source of the data to avoid multiplicity of storage and data protection costs. Nevertheless, real-time or velocity of data serves to provide higher values than veracity of data during a 'market crash'. "T+5 days" regulatory access means unproductive **idle time wasted** to take timely action in curbing potential abuse, protecting investors, and/or regulating an abnormal market event. **Prior to addressing these wastages, it is unfair and premature to ask for funding of this CAT**.

The outdated design of CAT with all the non-essential data 'at-rest' and 'in-motion' makes it more vulnerable to security threats than modernized RTAP. **Data-vault, data-lake, and 'golden source of data' are indeed attractive targets for**

---

[9] https://www.law.cornell.edu/constitution/fourth_amendment
[10] https://www.justice.gov/Overview_2020/download
[11] https://iapp.org/resources/article/state-comparison-table/ + G7 Cyber Exercise Programs + a new Bill has been introduced to the U.S. House Financial Services Committee on March 18, 2021 to prohibit the SEC from requiring that personally identifiable information be collected under consolidated audit trail reporting requirements, and for other purposes
[12] https://www.sec.gov/rules/final/2012/34-67457.pdf
[13] https://www.isixsigma.com/dictionary/8-wastes-of-lean/
[14] https://www.databoiler.com/index_htm_files/DataBoilerInMotion.pdf

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

hackers to treasure hunt. Hackers do not necessary come from outside; compromised internal executive(s) and staff(s) and contractors may pose even higher dangers because of potential cover ups and abilities to profit off any stolen data.[15] The Central Intelligence Agency – **Edward Snowden case**[16] is a prime example, i.e. **NOT a hypothetical "black swan"**[17] **cyber breach**. Additionally, the Director of National Intelligence has warned about China and Russia being the biggest threats to the U.S. in the latest assessment report.[18]. An insecure and breached CAT can cause the destabilization of the U.S. capital market, which trades in trillion dollars daily. **CAT must up its game for security protection against infiltration and foreign adversaries** or else it could become a threat to National Security.

The CAT NMS Plan **failed to address the following causes for potential information leak**: **Membership Inference Attacks**, **Reconstruction Attacks**, **Property Inference Attacks**, and **Model Extraction**.[19] It lacks scenario planning to counter different implementation of attacks (Centralized/ Distributed Learning). The trading and investment communities are concerned that **User Defined Direct Query and bulk extraction increase the vulnerability** of data being misused for impermissible purposes. We are not convinced that non-public data and PII will be safeguarded properly if measured against our suggested minimum requirements (please see *Table 1* of our November 30, 2020 comments[20] or *Appendix 1* in this letter). Without embedding appropriate analytical framework into the design of CAT as we have pointed out since our comments in 2016,[21] CAT may be a useless **gigantic vault that does nothing other than cause disturbances to all industry members** wasting valuable time and energy in data submission and causing worry about security and compliance.

Why would large Exchange Groups with robust surveillance systems and linked to market data feeds **at nanosecond precision need a "50± millisecond tolerance" CAT system?** "If" one would **play the devil advocate of using CAT data for non-regulatory purpose (i.e. function creep)**, CAT will not save Exchanges from subscribing to other peer Exchange feeds given the T+5 access for CAT, but what if these non-public data and PII offer valuable insights to help Exchanges target to attract order flow? Would countless buy and sell-side broker-dealers and market makers be cut-out from the industry value chain[22]?

CAT participants and industry members seem to address themselves to the parable of the **blind men and an elephant**[23] and/or hustle to seek shelter – immunity[1] and/or defer until "accommodate the unending demands of the industry"[24]. Frankly, the only parties that **stand to gain from an ever growing size of CAT** may be the vendors. These **cloud storage**, security, infrastructure, data processing vendors and other big law or compliance consultant firms **add layers of costs to the industry without adding much value to the monitoring and analytical aspects of CAT**, how sad!

B. Outside delegate authorities, NOT immune from risks/ liabilities claims

The proposed **limitation of liability provisions discourages CAT Participants from advancing the security protection** and design of CAT and CAT data. Although Self-Regulatory Organization (SRO) immunity may be broad, including affirmative acts and omissions and failures to act. SROs, however, do not enjoy complete immunity from suits. According to these

[15] https://www.linkedin.com/pulse/big-data-privacy-security-control-kelvin-to/
[16] https://www.britannica.com/biography/Edward-Snowden
[17] https://www.sec.gov/comments/4-698/4698-8573527-230862.pdf
[18] https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf
[19] https://arxiv.org/pdf/2007.07646.pdf
[20] https://www.databoiler.com/index_htm_files/DataBoiler%20SEC%20CAT%20Enhanced%20Security.pdf
[21] http://www.databoiler.com/index_htm_files/DataBoiler%20CAT613%20Comments.pdf
[22] https://www.linkedin.com/pulse/smile-curve-changes-securities-value-chain-evolves-kelvin-to/
[23] https://en.wikipedia.org/wiki/Blind_men_and_an_elephant
[24] https://www.sec.gov/comments/s7-10-20/s71020-8077540-226001.pdf

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

court cases,[25] FINRA and presumably all SROs **remain subject to liability** should **claim(s) arises as a result of private business or commercial conduct**. The **SROs' immunity from private civil actions applies ONLY when they are acting within their delegated authority**.[26] How courts apply a "functional test" to determine whether an SRO is entitled to immunity from burdens of litigation or civil damage suits may be a controversy here. If in the case of SROs' executive(s) or staff(s) or contractor(s) **willful misconduct, gross negligence, bad faith or criminal acts** related to CAT, SROs **should NEVER be immune** under those circumstances because these are **not part of their arbitral and prosecutorial authority**. Given FINRA replaced Thesys Technologies (a private company) as the CAT processor indeed signified that FINRA and CAT LLC are in effect **conducting private business.** We argue **such commercial conducts must subject to corresponding risks and civil claims in the case of liability**.

When we rebut the Charles River Associates' Economic Analysis (CRAEA) on their estimates of "greater than $100 million damage or 95% percentile loss may misguide policy makers info **falsely believing the risks may possibly be accepted when it should not**" in our January 27, 2021 comments.[27] We are thinking of the temptation for function creep[28] and the realism of various **adverse scenarios**[29] **if happened to CAT may potentially destabilize our capitalistic system and economy**. On the other hand, we have the following picture in mind:

Outsized risks of this elephant cannot be accepted, insurers refuse liability coverage.

CAT participants seek immunity and ways out by transferring risks to Industry Members.

Industry Members cannot absorb the risk and has no way to mitigate risks outside of their controls.

Shouldn't this be a CAT, not an Elephant in the first place? What can be done to ensure fit-for-purpose and proper security protection, so risks would be mitigated accordingly rather than being forced to accept or unnecessarily transferring the risks to ordinary investors that have nothing to do with risky or abnormality of trading activities.

[25] Weissman v. Nat'l Ass'n of Sec. Dealers, 468 F.3d 1306, 1312 (11th Cir. 2006); see also Sparta Surgical Corp. v. Nat'l Ass'n of Sec. Dealers, 159 F.3d 1209, 1213 (9th Cir. 1998).

[26] https://lawreview.uchicago.edu/sites/lawreview.uchicago.edu/files/77-2-SRO Immunity-Nafday.pdf

[27] https://www.databoiler.com/index_htm_files/DataBoiler%20SEC%20CAT%20Limitation%20Liability.pdf

[28] **The defined purposes of accessing CAT should be much narrower** than the broadly defined "regulatory purposes". Using tax filing to the Internal Revenue Service (IRS) as an illustrating analogy, the IRS asks for income information, but would not ask for the complete customer and supplier lists and detail transactions unless the party is being summoned in court. Therefore, we argue that there should be **no access to CAT** for 'market surveillance' purpose **prior to identifying symptoms of irregularity that are substantiated** by data at Securities Information Processors/ Competing Consolidators and/or analytical procedures at SROs/ the SEC.

[29] The **CRAEA failed to account for scenario, such as the Edward Snowden case** where information from CIA systems got exposed to WikiLeaks. The CRAEA also neglected the scenarios, such as the **2015-2016 SWIFT banking hack**, where hackers used stolen information of a foreign central bank to initiate the scam/ scandal to theft on the Federal Reserve Bank of New York; or **Market Chaos** such as the **GameStop phenomenon** if it may allegedly involve foreign adversaries. We can go on-and-on with additional scenarios and potential exploitations or abuse of CAT. In any case, the SEC's proposed standard Limitation of Liability Provisions (LLP) to the Reporter Agreement and Reporting Agent Agreement is **inconsistent with the Exchange Act** because **these threats could escalate into National Security issues which are outside the jurisdiction of the SEC**.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

Nevertheless, neither the SEC nor the SROs have rights above the U.S. Constitution. Please be reminded that the **Fourth Amendment right to be free of unwarranted search or seizure**, recognized by the Supreme Court as protecting a general right to privacy.[9] No-one wants his/her data be used by regulator(s) to develop policies that potentially may discriminate against him/her. **Suspicion of crime or anticipation of market turmoil should begin with some basis or require 'search warrant'** before permissible collection or surveillance on information that would otherwise be considered as private. Unlike census, collection of non-public and PII by CAT for all trade activities without express consent by the investors is an intrusion of one's privacy. **Stakeholders of CAT should NOT be placed above the law**.

According to a recent National Security Commission on Artificial Intelligence Final Report[30], "The reach of tools that China, for instance, uses to monitor, **control, and coerce its own citizens**—big data analytics, surveillance, and **propaganda**—can be extended beyond its borders and directed at foreigners. **Without adequate data protection**, A.I. makes it harder for anyone to hide his or her **financial situation**, patterns of daily life, relationships, health, and even emotions. **Personal and commercial vulnerabilities become national security weaknesses** as **adversaries** map individuals, networks, and social fissures in society; predict responses to different stimuli; and model how best to **manipulate behavior or cause harm**. The rise and spread of these techniques represent a major counterintelligence challenge."

This is America, not a communist country that performs **massive government surveillance**.[31] To be consistent with §11A or any other provision of the Securities Exchange Act of 1934, we think the SEC has full authority to pursue, without worry of other U.S. regulatory authorities' objection, to **demand better Suspicious Activity Report** (SAR) from Broker-Dealers (BDs) and/or **order improvements** of BDs' trade controls or fulfill certain compliance requirements. We also think **the SEC has rights** (without stepping on other agencies' jurisdictions) **to adopt the "A-Z" clauses** that we suggested in *Appendix 1*, as part of the minimum requirements for CAT NMS Plan's principle based rules rather than the Enhanced Data Security proposal which makes specific reference to an outdated revision 4 of SP800-53 by the NIST.[8] However, the CAT NMS Plan in its current form or the application of the captioned proposal(s) may be in **contradiction with the Department of Justice's** latest edition of the **Privacy Act of 1974**[10] and other applicable laws and new bills[11].

C. CAT's Funding does NOT have to be a "Sh*t hit the fan" scenario, there are better alternatives

At Data Boiler, we despise the mentality of stop trying when there is still room for improvement. Attempt to **"allocate" risks (shift liability disproportionally) to industry members** who are **NOT users of CAT** and have **NO control over** potential security breach caused by CAT participants, external hackers, or in case of CAT system failure is **UNFAIR**. If we compare the current CAT design with our "A through Z" requirements per *Appendix 1*, we see **significant deficiencies and ineffective controls requiring immediate attention**. We are not sure if that's the reason why the CAT operating committee seems to hesitate to respond to each of our 26 suggestions[17], but **to resolve CAT's challenges, it takes not just cooperation and collaboration, but development and deployment** efforts.

CAT participants and Industry Members do not have to worry about heightened costs related to improving CAT's system and security and privacy controls, because creative design such as **our alternative suggestions** per *Figure 2* of our November 30, 2020 comments or *Appendix 2* in this letter, would innovate the approach to analyze suspicious trading behavior and unusual market events directly and quickly, as well as **yield substantial savings while enhancing security for all parties**. In turn, the essential data stored at CAT would be much more manageable, data control would be more robust, and **by then, insurers should be more willing to provide liability coverage**.

[30] https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf
[31] https://en.wikipedia.org/wiki/Mass_surveillance_in_China

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

Regarding CAT's **funding model**, **both the original and the revised proposal are like the Financial Transaction Tax** (FTT).[32] The plan is simply **tolling everyone** in the industry, which will ultimately be passed-down to the end-investors. We question why the CAT operating committee, a CAT governing body composed of ONLY representatives of the SROs, would hold **concentrated power** on the **Funding Authority** as set out in §11.1?[33] **We challenged the Article XI §11.2 Funding Principles being insufficient to check against the CAT operating committee's legislative power** to (a) approve budget of CAT and (b) establish fees for themselves as well as for all industry members, the committee's **executive power** in (c) imposing and collecting of all Consolidated Audit Trail Funding Fees, and the **judicial right** to (d) assign and change the tier assigned to any particular Person, resolution of disputes upon reasonable notice to such Person. Even though the SROs are required to file the fee schedules with the Commission, such **unchecked power**[34] **of the CAT operating committee** would not ease the public or the industry community's concerns for **potential biases**.

If the CAT operating committee's funding authority under Article XI §11.1 is a delegated power conferred by the SEC to perform a **public** duty, then we have the following concerns and/or questions:

i. Bifurcated Cost Allocation is Inequitable and Proposed Minimum for Industry Members

Why are the CAT fees not imposed on the direct recipients of those that receive benefits from such services but rather a **'tax' on all industry members**? Whether CAT participants should or should not be the direct recipients of CAT benefits is also arguable given the rationale we stated in Part A of this letter.

a) If the CAT fee is related to supporting the **SEC** to "rapidly reconstruct market events/ trading activity" **beyond using the public available data**, then the Commission may subscribe to the SROs' proprietary feeds for any non-public data, or seek expressed consent to voluntarily share, or use of its permissible authority to summon the relevant private information.

b) If the CAT fee is related to "facilitating risk-based examinations" and/or "**improving abilities** for evaluating tips, complaints and referrals of potential misconduct made to regulators, monitoring and evaluating changes to market structure", then the **SEC and SROs** may **go back to the Congress for funding** or pay for it using collected **fines, penalties**, and intragovernmental fees, but not "user fees".

c) If the CAT fee is related to "better identification of potentially manipulative trading activity, increased efficiency of cross-market and principal order surveillance", then **private surveillance businesses affiliated with Exchange Groups** stand to receive benefits from CAT, hence they should pay the most if not all of such CAT costs. The **SEC** and **other SROs shall have choice** to use peers' surveillance system, or build their own or buy from other private vendors.

d) If the CAT fee is related to "improving efficiencies from a potential **reduction in disparate reporting requirements and data requests**", then it should be segregated into regulators' portion and the users' portion. **If** CAT is constituted as one of the "**user fees**" **imposed by the SEC and/or SROs**, then according to the Government Accountability Office (GAO), these "fees assessed to users for goods or services provided by the Federal Government are **deposited to the Treasury** as miscellaneous receipts and are generally **not available to the agency**."[35]

---

[32] https://securitytraders.org/wp-content/uploads/STA-FTT-Letter-FINAL-03_16_2021.pdf

[33] https://www.catnmsplan.com/sites/default/files/2020-02/34-79318-exhibit-a.pdf

[34] https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/6/1038/files/2015/10/leadership-xtufp4.pdf

[35] Fees assessed under the authority of the Independent Offices Appropriation Act of 1952 (codified at 31 U.S.C. § 9701), rather than under a specific authorizing statute, must be deposited to the Treasury as miscellaneous receipts and are not available to the agency or program that collected the fees, unless otherwise authorized by law.

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

If the SROs argue that CAT fee setting, collection, and dispute resolution are common commercial practices that they should have full discretion, then, CAT would not be part of their arbitral and prosecutorial authority. Hence, the SROs **should not enjoy immunity** related to their **private businesses** and the **industry members shall then have choice** (under antitrust laws), including **rights to opt-out** of CAT given they are not even users of the CAT system. **If** CAT fee/ minimum is a "**pay to play**" bundled cost to participate in a market, then this "tax" is a **barrier of entry inconsistent with** the competition, capital formation, and other goals of **the Exchange Act**.

ii. The allocation and minimum are undue burden on Industry Members

Other than a negotiable portion of point "C(i)(d)", **CAT has no reason to allocate an inequitable**[36] 75% of **CAT cost to Industry Members**. **The proposed $125** per quarter ($500/ annum) **minimum** to Industry Members hits 225 industry members in the bottom population (18.2% of 1237). There will be 792 industry members (64%) paying 1 penny to 86 cents above the minimum per quarter under the proposal. If counting from industry members #37 to the #1237 (**97.1%**), they **generate 3.33% of message traffic**, but will be **required to pay for 4.26%** of aggregated industry member fees under the proposal. It is a huge wastage in CAT billing and other administrative functions to **collect these "de Minimis" fees** or minimums from small industry members; it proves that the proposed funding model is **inconsistent with funding principle §11.2(d)**.

Also, why should **smaller firms subsidize the top** 36 elites whom generate 96.67% of message traffic but will pay 95.74% of aggregated industry member fees after the discounts? Some of the top elites already receive 32 mil super-tier rebates and other favorite treatments to compensate for their market making efforts and order flow contributions in the price discovery process. The **CAT operating committee's proposal with discount, maximum cap, minimum, and other adjustments** would further **exacerbate the inequalities in the market**[37]. Establishment of funding model without involvement of industry members and the public may raise public concerns or potential negative impression that CAT being a "private party" among elites to seek unfair advantages over others. Contrast to serving the public interest, rulemaking to seek sole benefit for the government agency or the affiliated SROs should be prohibited.

We **suggest adding a new CAT funding principle 11.2(g)** about CAT costs allocation should be **in proportion with specific public benefits received**, i.e. not private benefits of CAT participants; and those that have higher **implicit risk and vulnerability to potential conflicts of interest** must be charged higher fees than others, **to cover what is not already funded by fines and settlements** from abuse or other securities law violation cases.

iii. Proposed CAT Participants allocation versus Our Counter Suggestions

We argue against both the original "execution venue" concept and the proposed "message traffic" concept. If CAT NMS Plan is meant to prevent future flash crashes, curb suspicious trading behavior and unusual market events, then **why should one who is doing things fairly and squarely be subjected to regulatory scrutiny and CAT cost burden? CAT funding model should be driven mainly by fines and settlements**. We believe the Commission's current operating cost is also supported substantively by fines and settlements. So fines and settlements should be deemed acceptable revenue streams to cover CAT LLC costs satisfying the Article XI §11.2 funding principles.

If fines and settlements are insufficient to cover all CAT costs, then the SEC and CAT operating committee may consider imposing a negotiable portion of an earlier mentioned point "C(i)(d)" cost to those **based on materiality**

[36] https://www.sec.gov/tm/staff-guidance-sro-rule-filings-fees
[37] https://www.linkedin.com/pulse/animal-farm-market-data-negotiate-more-equal-kelvin-to/

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

and number of suspicious activities reported on the Suspicious Activity Reports (SAR). Those who under report on SAR should get increased fines. We think those **who "operate at the edge" and have higher risks for potential conflicts of interest, should bear much** of CAT cost given the extra efforts in deciphering their complex activities as compared to firms with a simpler business model. Indeed, **smaller players** who do not accept or pay payment for order flow (PFOF) and who are not entitled to access fee rebates **deserve appropriate subsidies**, so there will be a sustainable pipeline of emerging broker-dealers to participate in the markets.

a) Categorization of ATS, Market Making Discount, and Maximum are Unjust
Regarding Alternative Trading Systems (ATS), we think Dark pools introduce higher implicit risks due to their lack of transparency and vulnerability to potential conflicts of interest[38] than Lit venues. Therefore, **dark pools** should bear higher CAT cost than SROs. That being said, **internalizers / market makers** may post higher risks and be more vulnerable to potential conflicts of interest[39] than Dark Pools. Equity / Option Market Makers whom **business model derive from paying substantial rebates to others should NOT get a CAT discount**. Whereas **Tier 2** and smaller Market-Makers **whom do not pay or receive any rebate** have a simpler business model and **deserve appropriate subsidie**s to encourage their participation.

The SEC should **scrutinize industry members who are owners/ affiliates with ATS, or sponsors to an Exchange** to **avoid potential exploitation** of their economy of scope or **alleged trading cartel** in price setting or allocation of disproportional incentives. Again, **more CAT cost should be allocated** to those requiring regulators **extra efforts in deciphering** their complex activities as compared to firms with a simpler business model. **SAR would be a good basis for easier administration** in determining CAT fees.

b) Capitalize on 'Historical Assessment' (Thesys past development work) or is it a sunk cost
Why should the public (industry members would ultimately pass down the cost to end investors) **pay for anything** (recover 75% or ~$145 million incurred in Period 1) that may be allowed to **capitalize on as** the CAT LLC/ FINRA/ CAT Operating Committee's "**private asset**"? **If** past development work by Thesys is considered as "**public asset**", then why **wasn't there a full disclosure of all CAT's budgeted building and operating costs** for the public to review before the incurrence? **If** it is a "**sunk cost**", **why should industry members bear consequences of procurement decisions** that they were not part of the approval process, and are not and will not be 'users' of the CAT system?

c) Troubles in excluding OTC in Equity/ Listed Option Group Spit for CAT Participants
We acknowledge that FINRA being a **non-profit** trade association managing the trade reporting facility (TRF) for Over the Counter (OTC) products rather than a for-profit Exchange may have a **harder time to shoulder CAT burden**. **Yet, FINRA replaced a private vendor** Thesys as the CAT processor and **should not get preferential treatment** based on its non-profit or SRO status. Although we acknowledge that the nature of OTC trading in penny level may inherently be different from the proposed message traffic measurement use in Equity / Listed Option Group Split, similar arguments may apply to thinly traded securities, ESG stocks, etc., which SEC rule **should avoid "craft-out"**.

OTC has **high implicit risks due to lack of transparency and vulnerability to potential conflicts of interest**[40] than Equity and Listed Option asset class. And for the fact that FINRA would receipt explicit benefit from CAT

[38] https://www.ft.com/content/98e9b691-291f-3ef6-a917-cf27587b4ff5
[39] https://www.thetradenews.com/baml-slapped-second-time-42-million-fine-masking-orders/
[40] https://libertystreeteconomics.newyorkfed.org/2020/01/how-does-information-affect-liquidity-in-over-the-counter-markets.html

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

(from perspectives of being the CAT processor, may capitalize prior development works by Thesys, and CAT will enhance FINRA's technology[41]), FINRA as a **direct recipient of CAT benefits must bear higher portion of CAT costs** than other SROs whom do not own or affiliate with a surveillance business. Indeed, FINRA and its cloud vendor – FINRA and Amazon Web Services (AWS) should fend off any public concerns about **too big to fail** (TBTF) by voluntarily **providing full disclosure**, and the SEC should scrutinize, to ensure **CAT funding won't be mixed-in cross-subsidizing** existing surveillance and cloud processing business. There is a thin line between synergy and potential conflicts of interest (especially, FINRA also holds the SRO power to fine broker-dealers over surveillance system deficiencies[42]). We oppose the proposed FINRA-related cap allocation/ reallocation "Adjustment" and any Equity/ listed option Market Makers Discounts.

It is worth mentioning that CAT participants included Listed Options Venues and is **missing Futures and SWAP data** is one of CAT's biggest flaws. Thus, making this "gigantic vault" useless for meaningful market analysis.

d) Opposing the proposed Market Share approach to replace/ eliminate tiered fixed fees
To preserve the equitable, non-biased, fair, and non-discriminatory principles and fend off any public concerns or potential negative impression of CAT being a "private party" among elite CAT participants with fee cap, maximum, and adjustments, we again **suggest adding a new CAT funding principle 11.2(g)** about CAT costs allocation should be **in proportion with specific public benefits received**, i.e. not private benefits of CAT participants; and those that have higher **implicit risk and vulnerability to potential conflicts of interest** must be charged higher fees than others, **to cover what is not already funded by fines and settlements** from abuse or other securities law violation cases.

D. Other remarks and Conclusions

The CAT operating committee's proposals if adopted will put undue burden on good industry members and is not a deterrent to those industry members who introduce risk and **detriment to the public interest**. It will have an **adverse impact on the incentives of the CAT participants to ensure the security of CAT and CAT data**. These proposals will NOT remove impediments to, and will NOT perfect the mechanisms of the NMS, will NOT furtherance of the purpose of the Exchange Act, but would exacerbate the **potential exploitation of powers** allegedly by the CAT Participants leading to **inequitable, biased, unfair, discriminatory** situations harming smaller industry members, putting burden on competition, and may destabilize the fairness and orderly markets. We want to emphasis that we despise "kicking the can down the road". The **civic concerns** about **Massie Government Surveillance** should not be treated lightly. According to M.I.T. professor Gary Marx's statements in this Stanford University's study[7],

> *"…most people in our society would object to this solution, not because they wish to commit any wrongdoings, but because it is invasive and prone to abuse … fails to take into consideration a number of important issues when collecting personally identifiable data or recordings … such practices create an archive of information that is vulnerable to abuse by trusted insiders … In addition, allowing surreptitious surveillance of one form, even limited in scope and for a particular contingency, encourages government to expand such surveillance programs in the future. It is our view that the danger of a 'slippery slope' scenario cannot be dismissed as paranoia …"*

[41] https://www.finra.org/about/technology
[42] https://financefeeds.com/finra-fines-lime-brokerage-surveillance-system-deficiencies/

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

We disagree with the authors of the CRAEA because their three types of breaches scenarios are insufficient to represent the **potential damages to our country's economy and national security** in case of a breach. Captioned releases of CAT NMS Plan amendment proposals are inconsistent with §11A of the Exchange Act, the **Fourth Amendment of US Constitution**[9], the Department of Justice's latest edition of the **Privacy Act of 1974**[10] and other applicable laws and new bills.[11] Hence, we assert that **the SEC should disapprove these CAT proposals**.

We **suggest adding a new CAT funding principle 11.2(g)** about CAT costs allocation should be in proportion with specific public benefits received, i.e. not private benefits of CAT participants; and those that have higher implicit risk and vulnerability to potential conflicts of interest must be charged higher fees than others, to cover what is not already funded by fines and settlements from abuse or other securities law violation cases. Suspicious Activity Reports may be a good basis to account for a negotiable portion of the CAT fee applies to industry members if it is related to "reduction in disparate reporting requirements and data requests"; those who under report on SAR should get increased fines.

CAT has an **Outdated Design**, is an **Outsized Elephant**. National security and privacy ordinance matters are **Outside Jurisdiction** of the SEC and the SROs to make sole determination. The unbearable building and on-going operating costs of CAT **Outweigh its Benefits**. CAT's development and deployment should not be a sprint, we must be persistent and thoughtful, and we must not give up to pursuit the very best approach with perseverance. **We hope our "win-win" solution** as stated in Appendix 1 and Appendix 2 **will help** everyone **charging forward on CAT** and receive bipartisan support. Feel free to contact us with any questions. Thank you and we look forward to engage in any opportunities where our expertise might be required.

Sincerely,

Kelvin To

Founder and President

Data Boiler Technologies, LLC

Former member of Financial Services Roundtable – BITS (Banking Policy Institute) information security committee

CC: The Honorable Gary Gensler, Chairman
The Honorable Hester M. Peirce, Commissioner
The Honorable Elad L. Roisman, Commissioner
The Honorable Allison Herren Lee, Commissioner
The Honorable Caroline A. Crenshaw, Commissioner
Ms. Christian R. Sabella, Acting Director, Division of Trading and Markets
Mr. Peter A. Winn, Acting Chief Privacy and Civil Liberties Officer, Department of Justice
Mr. Paul Neff, Director of Cyber Policy, Preparedness and Response in the Office of Cybersecurity and Critical Infrastructure Protection. Department of Treasury

This letter is also available at:
https://www.DataBoiler.com/index_htm_files/DataBoiler%20SEC%20CAT%2020210503.pdf

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

Appendix 1

Below showcases the 'A through Z' security and privacy clauses that we recommend the SEC to adopt these clauses as part of the minimum requirements for principle based rules instead of the "problematic" enhanced data security proposal.

#	Suggested Clauses	Rationale/ Justifications
A	CAT should minimize 'data-in-motion' whenever and wherever possible;	The more frequent the transmittal of data in-and-out and within CAT, the more vulnerable it is.
B	Whenever and wherever the data is consumed or 'in-use', it has to serve 'defined purpose(s)' and be at a 'secured environment';	Civic concern of massive government surveillance. 'Data-in-use' is more vulnerable than 'at-rest'. The more users/ devices access to data, the greater the risk hackers may alter/ add/ insert/ use the data abusively.
C	The appropriate eradication or removal of data as soon as data has been transmitted or used to avoid 'function creep';	Omission or incomplete or untimely eradication would introduce opportunities for hackers.
D	No usage or possession outside of 'defined purposes';	'Function creep'[43] = abuse of CAT related tech or data.
E	When data is 'at-rest', it must be stored at designated 'secured environments';	Data-vault, data-lake, and 'golden source of data' are indeed targets attracting hackers to treasure hunt.
F	'Secured environments' must be segregated in accordance to 'sensitivity' of stored data;	Minimize vulnerability to specific range of data fields and/or records.
G	If data is considered 'sensitive', it must be obfuscated at all times ('at-rest'/ 'in-motion') except when it is 'in-use'; whenever 'alternate' surveillance methods are available, CAT users should refrain from querying 'sensitive' data.	Personal identifiable information (PII) or any data similar to that nature is deemed sensitive. If there is a way(s) to enable surveillance intelligence[44] without crossing the line of privacy[45] hazard, CAT must adopt.
H	'Defined purposes' are limited to 'market surveillance', 'specific case investigation' and/or 'rule enforcement' only;	Again, the Civic concern as stated in "B". No-one wants his/her data be used by regulator(s) to develop policies that potentially may discriminative against him/her.
I	If using metadata can achieve the 'defined purpose', CAT should by all mean avoid collecting or creating repetitive copies of raw data;	Prevent information leakage. Somehow metadata is more useful than raw data, especially when raw data is inherited with imperfect quality (50±ms tolerance).
J	If using 'integrated' data can achieve the 'defined purpose', CAT should avoid collecting data at lower domain;	Roll-up aggregation is another technique similar to masking or obfuscation that helps prevent leakage.
K	All data trajectory must be mapped, assessed, and monitored;	Scrutinize any Repurpose or Reuse or Recycle of data.
L	All users' entitlement in accessing CAT or its data must be duly authorized and maintained without delay;	Share access is a common threat, and lapsed entitlement introduces opportunities for hackers.
M	No access to CAT before a 'defined purpose' is identified and a secured connection is established;	Access entitlement does not mean there is no usage limit on CAT. Gateway and proxies need appropriate inspection to deter unsecure connection to CAT.

[43] When data is collected, whether such data remains used for its stated purpose after its collection has been called into question… even when two databases of information are created for specific, distinct purposes, in a phenomenon known as 'function creep' they could be combined with one another to form a third with a purpose for which the first two were not built… This non-uniqueness and immutability of information provides great potential for abuse.

[44] https://people.eecs.berkeley.edu/~jfc/mender/IEEESP02.pdf

[45] https://www.fdic.gov/regulations/examinations/financialprivacy/handbook/

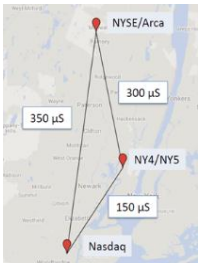
☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

#	Suggested Clauses (continue)	Rationale/ Justifications
P	Whenever possible, apply analytic techniques closest to the original source of data rather than making redundant copies of data;	Redundant copies of data affect data quality and expose the information to higher chance of unauthorized access.
N	All user activities must be logged timely in the system;	For scrutinization of any abnormal activities.
O	CAT functionalities and 'data-in-use' should be segregated based on 'defined purpose(s)' of specific user group(s);	Restrict the usage to specific range of data fields and/or records that fits the 'defined purpose(s)'.
Q	Use of 'predefined automated analytical steps' instead of ad-hoc data query wherever possible;	'Predefined automated analytical steps' require proper testing and authorization by Operating Committee.
R	Volume and frequency of ad-hoc data queries for 'specific case investigation' or 'rule enforcement' purpose is limited;	E.g. to < 0.001% of daily order volume of the targeted broker-dealer with suspicious activity per-query per-user per-day; < 0.01% in aggregate every two weeks.
S	No access to CAT for 'market surveillance' purpose prior to identifying symptoms of irregularity that are substantiated by data at SIPs and/or analytical procedures at SROs/ the SEC;	Again, the Civic concern as stated in "B". Suspicion of crime or anticipation of market turmoil should begin with some basis or require 'search warrant' before permissible surveillance on information that would otherwise be considered as private.
T	Bulk data extraction is generally prohibited, except during 'market crash' with special authorization from the SEC;	Where 'market crash' period may refer to Limit Up-Limit Down trigger or exchange halt scenarios.
U	Database server infrastructure and configuration should prioritize 'consistency' and 'partition tolerance' over 'availability', and CAT system should be in compliant with Atomicity, Consistency, Isolation, and Durability (ACID).	The controversy is that CAT as a surveillance tool is supposed to prioritize 'availability' over the two other attributes. Real-time or velocity of data serves to provide a higher values than veracity of data during a 'market crash'. The T+5 access defeats CAT purpose.
V	Data loss protection (DLP) infrastructure must include proper steps for effective and efficient data disposal;	Retaining more data than necessary is a liability. Record retention must be enforced diligently.
W	Audit logs (including user activities, network performance and other system gauges for automated threat detection) must be readily available for exam upon request;	The timelier the review, the higher the chance to salvage a loss situation.
X	Abnormality to CAT or its data or connectivity, or breach of control must be reported in timely manner;	Give the reviewers the authority to provide non-bias and timely report of problems to the upmost Seniors.
Y	Any control compromised must be diligently rectified; independent assessment to recommend interim actions;	Avoid 'bandage' or temporary fix, or a fix in one area may inadvertently cause vulnerability in other area(s).
Z	Must actively observe, adopt and pursuit relevant information security and privacy best practices.	Continuous improvement, ensure forward looking (e.g. today's encryption will be obsoleted upon quantum).

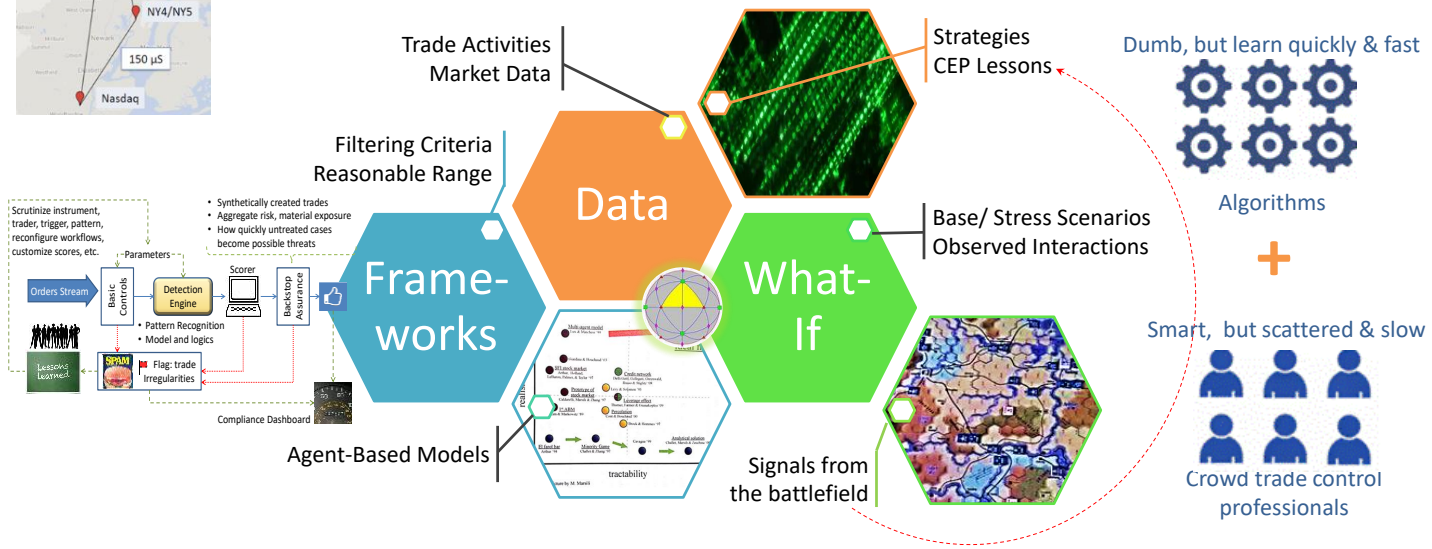
☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

Appendix 2

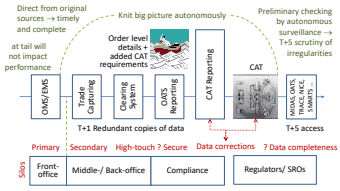
This innovative design draws analogy[46] to the IRS's successful 'my free tax initiative'; it would allow the SEC and CAT Participants to focus on those high-risk candidates for scrutinized exams. We envisage a crowd model to **reduce unknown unknowns**[47] **while enhance security of CAT**. The benefits of our suggested approach are: (a) dramatically reduce CAT footprint or data storage and traffic by avoiding unnecessary redundant copies of data and minimize 'data-in-motion'; (b) confine access to CAT data to 'targeted search' of relevant data that fits the 'defined purposes'; and (c) better intelligence for market monitoring by enabling and rewarding the crowd for identifying early warning signals to potential flash crash or other trade irregularities.



1. If SIPs will expand core data to include depth-of-book, odd-lots, auction, etc. (i.e. 'order level' details), then there is no need to overlap this publicly available information at CAT.
2. Cross tabulate early warning signals from mining of SIP data with intelligence gathered from SROs' surveillance systems (i.e. onset signal detection from better data (captured data at SIPs and SROs are at nanoseconds rather than CAT data with 50± milliseconds tolerance).



3. Enabling the crowd with an open platform consists of: (a) a community library of basic trade patterns, similar to a music editor tool for the crowd to modify basic patterns into new trade strategies to discover alpha (or the unknown unknowns), a simulation tool where new strategies will be back tested, and a reward scheme if back-testing results shown useful insights into reducing unknown unknowns.
4. By leveraging crowd intelligence in step 3 (learn from the field that is closest to the market and in real time) and combining with surveillance findings gathered from steps 1 and 2, it would substantiate enough supporting arguments for identified 'symptoms' of market or trade irregularities.



5. Then, whatever residual data that are not otherwise available at SIPs or SROs would be collected through CAT, which substantially reduces CAT storage (avoid unnecessary regurgitation or repetitive copies of data) to only those data that are essential for law enforcement or prosecution investigation related to specific cases.
6. Through pre-defined automated pre-screening of data that broker-dealers are about to submit to CAT (i.e. targeted to look for specific 'red-flag(s)'), if no 'red-flag' is found relevant to previously identified symptom(s), then trade activities may be certified 'clean' and that batch of data is no longer required to be stored at CAT.
7. With substantiated 'symptoms' and identified 'red-flag(s)', retrieve or subpoena evidence by querying relevant data field/ records would be permissible.

[46] https://www.linkedin.com/pulse/hr-block-analogy-cat-combating-fraud-kelvin-to/

[47] https://www.pmi.org/learning/library/characterizing-unknown-unknowns-6077