sifma
Invested in America

June 4, 2020

The Honorable Jay Clayton
Chairman
U.S. Securities and Exchange Commission
100 F Street NE
Washington, DC 20549

Re: ***Data Security Questions by Chairman Clayton on the Consolidated Audit Trail***

Dear Chairman Clayton:

The Securities Industry and Financial Markets Association ("SIFMA")[1] is pleased to offer input on the data security questions that you posed on March 17, 2020 to the Staff of the Securities and Exchange Commission ("SEC" or "Commission") regarding the consolidated audit trail ("CAT").[2] You have asked the Staff to consider these questions in connection with preparing a recommendation this year for the Commission on improving the data security requirements in the CAT NMS Plan ("Plan"). SIFMA has long supported the development of the CAT and believes that it will be a critical addition to the current market infrastructure, providing a significant resource to track equity and options trading activity across markets.

While the recent steps to protect certain personally identifiable information ("PII") of retail customers are designed to address significant, long-standing concerns, SIFMA continues to have serious concerns about the need for and security of customer data provided to and maintained in the CAT.[3] You and others have recognized more should be done by the self-regulatory organizations ("SROs") as the developers and operators of the CAT to protect the CAT Data maintained within the CAT System.[4] Keeping CAT Data secure and confidential is

[1] SIFMA is the leading trade association for broker-dealers, investment banks, and asset managers operating in the U.S. and global capital markets. On behalf of our members, we advocate for legislation, regulation and business policy, affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA).

[2] See Public Statement by Chairman Jay Clayton titled "Update on Consolidated Audit Trail; Temporary COVID-19 Staff No-Action Letter; Reducing Cybersecurity Risks" dated March 17, 2020 (https://www.sec.gov/news/public-statement/statement-clayton-cat-covid-19-nal-cybersecurity-2020-03-17).

[3] See Release No. 34-88393 (March 17, 2020), 85 FR 16152 (March 20, 2020).

[4] "CAT Data" and "CAT System" are defined in Article I, Section 1.1 of the Plan.

of primary importance not only to the efficacy of the CAT System itself, but also to the confidence of market participants. As SIFMA has stated previously, it is imperative that the CAT be held to the highest security standards and it is incumbent upon the Commission to ensure that those standards are clearly enunciated, established and implemented.[5] To that end, SIFMA is sharing with the Commission its input on the following CAT Data security questions posed to the Commission staff. We would very much appreciate receiving and reviewing the SROs' input on these questions as well to the extent they have provided such input.

Are there alternatives to "bulk downloading" data by each SRO that would better secure CAT data?

The security features of the Plan are outlined in Appendix D of the Plan. These security features for FINRA's CAT System include, among other things: (i) the encryption of PII and all other CAT Data, as well as a System Security Plan; (ii) adherence to the NIST 800-53 security standards, a set of security and privacy controls for federal information systems and organizations; (iii) incorporation of tools that will enable logging, auditing and access controls for the CAT System; (iv) secure methods of connectivity; and (v) development of a Cyber Incident Response Plan.

As noted, steps recently have been taken to protect the most sensitive PII of retail customers in the CAT. In particular, the Commission issued an order under which broker-dealers are now required to report to the CAT "phone-book" information regarding retail customers consisting of their names, addresses, and birth years, rather than more sensitive PII such as their social security numbers.[6] While the order tailoring PII in the CAT to "phone-book" data is a material improvement, SIFMA continues to believe there are better alternatives than collecting and maintaining PII in a customer data base in the CAT System from a data security and privacy standpoint.[7] Should the Commission allow for the development of the customer data base, SIFMA strongly believes that much more should be done to protect the sensitive data of market participants' customers that is transmitted to and stored within the CAT System. The same level of concern applies to the transaction database, given the vast amount of such data in the CAT System, the potentially thousands of individuals who could have access to such data and the types of potential conflicts that could arise at SROs related to access to this data. All of these considerations require CAT LLC and SROs as the Plan Participants to treat the CAT Data

[5] See Letter from Theodore Lazo, Managing Director and Associate General Counsel, and Ellen Greene, Managing Director, SIFMA to Brent Fields, Secretary, SEC dated July 18, 2016 (https://www.sifma.org/wp-content/uploads/2017/05/sifma-submits-comments-to-the-sec-on-the-nms-plan-for-a-cat-system.pdf).

[6] See supra note 3.

[7] See, e.g., Letter from Thomas Price, Managing Director, SIFMA to Brett Redfearn, Director, Division of Trading and Markets, SEC dated October 29, 2018; SIFMA White Paper titled "Consolidated Audit Trail - Alternative Approach for the Collection of Investor Personally Identifiable Information Leveraging the CAT Customer Identifier (CCID)" dated October 29, 2018; Letter from Thomas Price, Managing Director, and Ellen Greene, Managing Director, SIFMA to Jon Kroeper, EVP, FINRA dated August 13, 2018.

with the utmost degree of care and mitigate the attendant risks, as they are directly responsible for the CAT System and its security elements, and appropriately exposed to liability should the CAT System or CAT Data be breached as the developers and operators of the System.

SIFMA believes that an obvious and avoidable significant threat to the security of the CAT Data is the ability of SROs to bulk download customer and transaction data from the CAT to their own systems, including PII data. Such a process would remove the data from the CAT environment (with security measures in place) and place it in the hands of potentially multiple SROs and the individuals who work there. Rather than mitigating risk, bulk downloading would exponentially broaden the risk that the data could be exposed. It is inconceivable from a risk management standpoint that the Commission would allow bulk downloading customer and transaction data by 24 separate entities. In addition to the risk of PII exposure, for many types of market participants, exposure of transaction data could expose their sensitive and proprietary trading strategies and could allow, for example, competitors or bad actors to misuse data or reverse engineer their trading strategies. Among other concerns, these bulk transfers can subject CAT Data to additional abuses by bad actors, who have increasingly sophisticated methods of orchestrating cyber breaches, as well as expose SROs that bulk download and others to liability resulting from improper disclosure of sensitive trading data.[8] Indeed, for certain participants, it is not a stretch to say that they view their trading history with just as much importance as individual investors view their social security numbers. Thus, it is critically important that additional steps are taken to protect all CAT Data, including transaction data.

The current cross-market surveillance responsibilities for the equity and options markets reside almost exclusively at FINRA after having been outsourced by the exchanges to FINRA. In September 2017, the CEO of FINRA noted in a speech that FINRA had entered into Regulatory Services Agreements with 19 exchanges that operate 26 stock and options markets at the time of his speech.[9] FINRA's CEO further noted that through these agreements, and in coordination with the exchanges, FINRA's surveillance canvassed 99.5 percent of U.S. stock market trading volume and about 65 percent of U.S. options trading activity. In light of this regulatory landscape, it is unclear why or for what purpose exchanges would need to bulk

[8] We note that at a December 11, 2019 meeting between the SROs, SIFMA, industry representatives, and representatives from the SEC to discuss the CAT Reporter Agreement, a representative from Nasdaq indicated that Nasdaq does not plan to bulk download CAT Data, even though they have the authority to do so under the Plan. Similarly, the leadership of the SEC has indicated on multiple occasions that the SEC would not retrieve data from the CAT until it was certain that the information could be adequately protected. See, e.g., Public Statement by Chairman Jay Clayton titled "Statement on Status of the Consolidated Audit Trail," September 9, 2019 ("Further, with regard to the use of the CAT by the SEC, as I have previously noted, the SEC will not retrieve any PII from the CAT unless there is a regulatory need for the information and we are confident that there are appropriate protections in place to safeguard the in information.").

[9] See Speech by Robert Cook, President and CEO, FINRA titled "Equity Market Surveillance Today and the Path Ahead" dated September 20, 2017 (https://www.finra.org/media-center/speeches-testimony/equity-market-surveillance-today-and-path-ahead).

download data from the CAT, and to the extent there are specific use cases for why bulk downloading is necessary, it would be helpful to have a better understanding of them given the critical importance of protecting the CAT Data.

Currently, the Plan provides all SROs with the ability to bulk download CAT Data. As discussed in more detail below, SIFMA believes that allowing all SROs this ability presents enormous and unacceptable security risks related to the exposure of CAT Data. SIFMA further believes that any perceived need by SROs to be able to bulk download CAT Data is no longer justified because technology has evolved such that complex surveillance activities can be conducted within the CAT security perimeter.

SIFMA therefore believes, as it has stated previously, that the only way to address security concerns related to bulk downloading CAT Data by SROs is to prohibit SRO bulk downloading.[10] Based on the risk associated with bulk downloading CAT Data, all access to, and review of, more than a user-defined direct query of CAT Data should only be done in the CAT System maintained by FINRA CAT as the Plan Processor where strict access, entitlements, and other security measures can be employed by the Plan Processor. SIFMA therefore believes that further Plan amendments should be considered that would require that the SROs use a secure analytics workspace ("SAW") approach under which the SROs are required to access all CAT Data from within the CAT security perimeter, so that no such data ever leaves the CAT.[11] This would provide the regulators with access to perform (proprietary) surveillance runs in a secure and confidential manner without imposing the risk associated with bulk downloading data from the CAT.[12]

Further, the Plan should be amended to restrict each exchange's access to CAT Data in the SAW to provide that an exchange can only see data for trading activity conducted on that exchange (and not trading activity on other markets), with the only exception being for limited and well-defined regulatory purposes. As noted above, the current cross-market surveillance responsibilities for the equity and options markets reside almost exclusively at FINRA. As such,

---

[10] See, e.g., Letter from Kenneth Bentsen, Jr., President and CEO, SIFMA to the Honorable Jay Clayton, Chairman, SEC dated November 11, 2019 (https://www.sifma.org/wp-content/uploads/2020/01/SIFMA-Letter-to-SEC-Chairman-Clayton-on-CAT-Liability-and-Access-Issues-November-11-2019.pdf).

[11] SIFMA notes that the SAW was discussed in the following letter on behalf of the Plan Participants –Letter from Michael Simon, CAT NMS Plan Operating Committee Chair to the Honorable Jay Clayton, Chairman, SEC dated November 27, 2019 (https://www.catnmsplan.com/sites/default/files/2020-02/Simon-Letter-SIFMA-%28Final%29.pdf).

[12] SIFMA continues to be uncertain as to why appropriate database connectors cannot be employed to allow FINRA to conduct complex surveillance activities within the CAT security perimeter. If, however, FINRA is able to demonstrate to the Commission's satisfaction that it is not possible to conduct such surveillance activities in the CAT System, SIFMA believes that consideration should be given to amending the Plan to provide FINRA only with the ability to bulk download CAT Data to conduct such surveillance activities, subject to it also demonstrating that it meets or exceeds the security controls employed by FINRA CAT.

only FINRA should be provided the broad ability to access cross-market CAT Data in the SAW. Preventing SROs from bulk downloading CAT Data and limiting each exchange's access to CAT Data in the SAW are the best ways for the Commission to address the security concerns related to the ability of SROs to bulk download CAT Data.

What are the risks of proliferation of CAT data across multiple environments?

Once populated, the CAT will be the world's largest data repository of securities transactions, maintaining data on more than one hundred million customer accounts and their trading information. Due to the near-limitless possibilities to exploit such a rich data set by malicious actors, the CAT will stand as a large, valuable target for criminals, nation-states and other potential bad actors.

Bulk downloading CAT Data outside of the CAT System renders ineffective even the most advanced security measures that may be employed by the Plan Processor. In this regard, the risk of exposure of CAT Data increases exponentially when it is downloaded and stored in multiple environments outside the CAT System. For example, if 23 exchanges and FINRA are separately able to download CAT Data, the PII and trading information of millions of market participants would exist in 24 discrete environments. CAT Data would be placed at a significantly increased exposure risk due to the 24 SROs and thousands of individuals at them who would have access to such sensitive data. Even if bulk downloading is limited only to two or three exchange families, the risk of exposure of the data is significantly increased due to the number of environments in which the data would reside and the number of entities and individuals with access to the data. As the number of environments storing CAT Data increases, the burden of keeping this sensitive data secure increases. Moreover, it is worth noting that some of the exchanges that are CAT Participants are new entities that have launched within the last few years, and the newest Plan Participant is not even operational yet. As such, these organizations and their employees may not possess the same level of experience or sophistication as well-established SROs in dealing with data like that stored in the CAT, which could increase the vulnerability of such data to a breach.

Further, there does not appear to be a set of uniform or baseline standards among the SROs regarding their security controls related to the handling of bulk downloaded CAT Data. This lack of standards increases the risk of data exposure because it creates an environment in which the SRO with the fewest security controls or least experience could serve as the weak link that could be exploited by a malicious actor to access the CAT Data. This lack of standards also makes the SEC's oversight of the SROs' security controls more difficult and resource-intensive if multiple SROs have this ability. For these reasons as well as the ones noted throughout this letter, SIFMA believes that the Commission should eliminate the ability of the SROs to bulk download any CAT Data from the System.

Are there additional data security issues regarding the use of CAT data for regulatory purposes that should be addressed?

SIFMA strongly believes that the parameters regarding the appropriate use of CAT Data should be clearly defined in the Plan and not left open to interpretation. In this regard, one significant data security issue associated with the use of CAT Data among the exchanges is the potential that the data could be used for commercial purposes, which in turn could further jeopardize the security of the data. Currently, the ability of exchanges to access the trading data of other markets is constrained by a process in which as a general matter, one exchange's regulatory arm requests the data from another exchange's regulatory arm. These constraints, however, will no longer exist with respect to the CAT Data, as the CAT environment will allow an exchange to view the trading data from all the markets. Thus, the pressure to use such data for commercial purposes could increase dramatically, given the for-profit status of many exchanges. This could especially be the case if the exchanges were able to bulk download CAT Data, where its further usage could not be as effectively monitored as it could be if it were required to stay within the CAT System environment.

Furthermore, if bulk downloading is permitted, once the data has been downloaded by an exchange or FINRA, it is likely that the data would proliferate in multiple environments at the organization outside of the one in which it was downloaded. That is, once the data is inside an exchange or FINRA, employees and contractors may move or copy the data into other locations within the organization, in whole or part, for analysis and/or use. This further increases the risk of misuse of CAT Data. These are even more reasons why SROs should not be allowed to bulk download CAT Data from the System and exchanges should generally be limited to seeing only transaction data from their own markets.

Along these lines, further consideration should be given to spelling out in more detail the limited regulatory manner in which the CAT Data can be used by SROs. It is not currently clear under the Plan whether, for instance, the use of CAT Data by an SRO for a rule filing would be considered regulatory in nature in all circumstances. Although the rule-making process may generally be considered regulatory, many rule changes, and particularly those by exchanges, are commercial in nature since they are designed to attract more order flow to the exchange. For example, an exchange could decide that it would like to an institute a speed bump for incoming orders or a subset of incoming orders. If our recommendation to limit an exchange's access to transaction data in the CAT is not followed, the CAT Data from other exchanges could serve as a resource to the exchange regarding the performance and operation of speed bumps at those other exchanges. Although such use of CAT Data appears to be impermissible, clear parameters regarding the appropriate use of CAT Data should be set forth in the Plan. Even FINRA has certain commercial aspects, such as its trade reporting facilities that are alternatives to printing trades on exchanges. Accordingly, in addition to prohibiting bulk downloading and limiting an exchange's access to transaction data, the Plan should be amended to provide more detail on the appropriate regulatory uses of CAT Data by SROs.

If our recommendation to amend the Plan to unambiguously eliminate the ability of any SRO to bulk download CAT Data is not followed, to the extent any bulk downloading is permitted by the Commission, any CAT Data that is extracted from the CAT System by an SRO should be subject to strict and explicit data destruction practices once the use of the data has been completed.

How will access to customer and account information be addressed to restrict access to the greatest extent possible while still preserving the ability to achieve regulatory purposes?

In addition to prohibiting bulk downloading, as an overarching principle, only those SRO employees with a need to access CAT Data should have the ability to access it within the SAW. Further, access to customer data in the SAW should be provided only in the rarest of instances (*e.g.*, SEC investigations of securities law violations), as regulators and other authorized users should be able to perform the majority, if not all, of their regulatory responsibilities by utilizing non-customer data and/or by issuing direct data requests to market participants. In those limited circumstances where access to customer data is necessary, Role Based Access Control ("RBAC") with authorization subject to a "need-to-know" basis should be employed. FINRA CAT should have appropriate protocols in the SAW that govern the request for access and the approval process to gain such access. For instance, the protocols must require that it be clearly documented in advance what specific information the user is requesting and why that information is necessary. Should access be granted, the information returned must then be masked to return only the minimum amount of information necessary to fulfill the user's request. For instance, access to customer data in the SAW should incorporate a temporal standard that limits a user's authorization to the minimum amount of time necessary to perform such function.[13]

Moreover, appropriate policies and procedures should be in place for user access administration, including provisioning of administrators, user data management, password management and audit of user access management.[14] A federated authentication from the CAT Reporter / Authorized Reporting Agent should be leveraged (especially for those who have access to data they have not submitted); this will add to multi-factor authentication and allow for automated deactivation of users that leave such entities. There should be automatic deactivation for users who do not access the CAT for specified period of time (*e.g.*, 6 months), or whose access is not re-confirmed by their entity for 30 days during periodic access review, or whose firm account has been deactivated. The email address for CAT users should be immutable and should allow for change via administrative review workflow. Shared user IDs should not be

[13] If despite the significant security concerns the Commission permits bulk downloading of CAT Data by an SRO, it is critical that all of these controls noted above and below be followed in such a scenario.

[14] SIFMA believes that NIST Special Publication 800-53 should be considered in connection with assessing whether the access controls related to the CAT Data are effective.

allowed. Role-based access controls should be used to enforce appropriate separation of duties and avoid insecure user permission combinations. In addition, further detail should be provided regarding the process to terminate the access of off-boarded SRO staff to the CAT System and CAT Data. SRO staff who have access to the CAT System and Data in the SAW present potential significant security threats to the CAT System once they leave the SROs for which they worked. Accordingly, the immediate termination of their access rights should clearly and explicitly be provided for by the SROs.

In addition, SROs should be required to periodically review their access to and use of CAT Data in the SAW to ensure that the security measures they employ regarding the access to and use of CAT Data continue to be appropriately designed to meet current circumstances. The current work-from-home environment existing as a result of the COVID-19 crisis is a prime example of why this periodic review should be conducted, because it is very likely that the access to and use of CAT Data under these current circumstances would not have been contemplated six months ago. Moreover, FINRA CAT and the SROs should conduct behavior-based monitoring of the use of CAT Data by SRO employees as well as extensive tracking of access to such data by such employees.

Is oversight of Plan Processor security decisions effective and comprehensive?

SIFMA believes that additional measures regarding the oversight of the Plan Processor should be adopted. Currently, the Operating Committee of the Plan, which is comprised exclusively of SROs, serves as the governing body for CAT. It provides review, guidance, and oversight for the overall operations of the CAT and the Plan Processor. FINRA CAT serves as the Plan Processor, but it is also a subsidiary of FINRA and is provided certain services by FINRA pursuant to a shared services agreement. In this regard, for instance, the Chief Information Security Officer ("CISO") of FINRA CAT is a FINRA employee, although that individual is supposed to act in a fiduciary capacity with regard to the Plan.[15] The CAT also has an Advisory Committee consisting of industry representatives that provide the SROs with guidance and advice on the implementation, operation, and administration of the CAT, but the Advisory Committee has no voting power and the Operating Committee is under no obligation to follow its guidance with regard to the operation of the CAT.

The CAT NMS, LLC also has a Security Working Group ("SWG") comprised of the CAT CISO as well as CISOs and security experts from each Participant SRO. SIFMA understands that there are no member firms currently represented on the SWG. At a high-level, SIFMA thinks that a working group with member firm input could help enhance the security of the CAT by providing "best-practice" advice to the Plan Processor regarding security practices that work well at the organizations represented on the working group. In turn, it could also serve as a security resource to the organizations represented on the working group. As it stands today,

[15] See Presentation titled "CAT Security Overview – Safeguarding Data Reported to CAT" (https://www.catnmsplan.com/sites/default/files/2020-01/FINRA-CAT-Security-Approach-Overview_20190828.pdf).

however, member firms are not represented on the SWG and thus have very little insight into the qualifications of the working group members and the level of engagement the working group has with respect to CAT security. This is unfortunate given the significant level of expertise at member firms in protecting customer data. SIFMA therefore believes that the Commission should take a much closer look at the structure and operations of the SWG with the objective of enhancing its effectiveness, which could result in establishing a more targeted working group with industry member CISOs to assist the SWG much like was conducted to find a solution for collecting PII data.

As SIFMA has stated previously, the CAT should be governed in a transparent manner that delivers collaboration between the SROs and their members. To achieve this, SRO member firms must be integrally involved in the governance of the CAT with full voting rights. The current governance structure, which provides for the CAT to be governed exclusively by the SROs, does not appropriately provide a voice to the entities subject to the CAT requirements, namely the member firms. Such a governance structure is not optimal because it loses the input and expertise of this member firm group in areas where they have much to offer, including data security. Member firms with retail customer bases have been grappling with the protection of customer data for many years and have extensive expertise and experience that they could share in this regard. Moreover, if and when the SROs implement fees to pay for the development and maintenance of the CAT, it is critically important that the member firms have a say in this process. Indeed, the Commission recently recognized the critical importance in allowing member firms to have a governance say in an NMS plan as part of its order directing the SROs to amend the governance structure of the equity market data plans to include non-SRO representatives in the governance committee.[16] Accordingly, SIFMA recommends that the Plan be amended to provide for the representation of member firms on the CAT Operating Committee.

To what extent can there be additional transparency regarding the security of CAT and the use of CAT data without making the CAT system vulnerable to bad actors?

SIFMA recognizes that CAT is subject to Regulation SCI. As such, the CAT has an obligation to disseminate SCI events that are system disruptions and system compliance issues. SIFMA notes that satisfying this dissemination obligation is the baseline to demonstrate compliance with Regulation SCI, but nothing in the regulation prevents an SCI entity from reporting more than what is required. Indeed, given the nature of the CAT System and the information it contains, the reporting of system intrusions is the most critical and relevant information that can be shared with member firms that are CAT Reporters and Authorized Reporting Agents. While the CAT currently has no apparent obligation under Regulation SCI to do so, it is absolutely critical that firms be notified so that they can also take measures to protect their information that was compromised in the CAT System. SIFMA therefore requests that affected member firms that are CAT Reporters and Authorized Reporting Agents be notified of

[16] See Release No. 34-88827 (May 6, 2020), 85 FR 28702 (May 13, 2020).

such events in a timely manner. In addition, such member firms have significant experience in protecting sensitive customer information from attacks and can be an invaluable resource to the Plan Processor in such a situation. SIFMA emphasizes that it is not requesting that such intrusion information be made publicly available, but rather that it be shared directly with affected members so that appropriate measure can be taken.

SIFMA further requests that member firms be periodically apprised of the completion and results of any CAT-related security reviews conducted by the Plan Processor and SROs. This would include vulnerability testing as well as independent SOC 2 audits of data security and controls. Such a process would provide member firms with insight into the quality of security measures employed by the CAT and the SROs that have access to CAT Data. Moreover, such a process could allow member firms to offer valuable feedback in connection with the reviews. The reports could be tailored in such a way so that they do not expose sensitive security information to malicious actors. For instance, a high-level version of the report could be shared with a broader member firm audience that provides evaluation criteria and summarized results of reviews of CAT security practices and procedures without disclosing information that an attacker would use (*e.g.*, a third party firm conducted penetration testing against FINRA CAT in 1Q20 and only minor issues were reported, rather than a report detailing that a particular SRO uses a perimeter firewall that is missing a specific critical software update known to be regularly exploited by cyber attackers). A more detailed version of the report could be shared with the SWG as well as possibly a member firm working group related to the SWG. As it stands right now, member firms have very little transparency into the quality of day-to-day security practices of the Plan Processor and SROs regarding the handling of CAT Data. Providing periodic, summarized reports of security reviews to member firms could enhance the transparency and oversight of security programs and lead to enhanced confidence in the marketplace regarding the security of CAT Data.

Are there additional security measures that would enhance the security of CAT data, both within and outside of the CAT system?

SIFMA recognizes that CAT as an SCI entity has an obligation to periodically review its security posture in relation to current threats with the objective of making necessary updates to its technology and processes to protect against such threats. SIFMA requests that member firms that are CAT Reporters and Authorized Reporting Agents be notified of any anticipated major changes to systems, technology and architecture that are planned for the CAT as a result of such reviews. This would provide member firms with transparency regarding such changes and afford them the opportunity to provide valuable feedback regarding such changes. As noted, member firms have extensive experience in protecting sensitive customer data and could serve as an invaluable resource to the CAT.

Overall, SIFMA believes that following the approaches outlined above, and particularly the recommendation to eliminate the ability of SROs to bulk download CAT Data, can only help enhance the security of the CAT System and CAT Data. Again, in our strong view, allowing 24

SROs to bulk download data from the CAT is completely incompatible with mitigating cyber risk related to such data and places such data at an unacceptable risk of a breach. Further, the SROs and CAT LLC, and not our members, should bear any and all liability related to any breach of CAT Data once it is transmitted to the CAT. SIFMA notes, however, that these approaches are based on what member firms have learned to date about the practices and processes related to the security of CAT Data. There could be other, non-disclosed issues related to such practices and processes that also need to be addressed, such as the robustness of the encryption practices regarding any CAT Data at rest as well as in transit. That is one of reasons why the recommendations regarding heightened member firm involvement in the security of CAT Data are critical. Member firms have vast experience in handling and protecting sensitive customer data and increased input by the firms could significantly help bolster the overall security of CAT Data.

* * *

SIFMA greatly appreciates the Commission's consideration of input provided above and would be pleased to discuss it in greater detail with the Commission and its Staff.

With kindest personal regards,

Kenneth E. Bentsen, Jr.
President and CEO

cc: The Honorable Jay Clayton, Chairman
The Honorable Hester M. Peirce, Commissioner
The Honorable Elad L. Roisman, Commissioner
The Honorable Allison Herren Lee, Commissioner

Bryan Wood, Deputy Chief of Staff
Manisha Kimmel, Senior Policy Advisor to the Chairman
Brett Redfearn, Director, Division of Trading and Markets