sifma
Invested in America

November 30, 2020

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

Re: ***File No. S7-10-20; Amendments to the National Market System Plan Governing the Consolidated Audit Trail to Enhance Data Security***

Dear Ms. Countryman:

The Securities Industry and Financial Markets Association ("SIFMA")[1] respectfully submits this letter to the U.S. Securities and Exchange Commission ("SEC" or "Commission") to comment on the above-referenced proposed amendments (the "Proposal") to the NMS plan governing the Consolidated Audit Trail (the "CAT NMS Plan" or "Plan").[2] The Proposal is designed to strengthen the security and protections for data in the Consolidated Audit Trail ("CAT") and to limit the scope of sensitive information required to be collected by the CAT.[3] SIFMA has long supported the development of the CAT and believes that it will provide a critical market infrastructure resource for regulators to track equity and options trading activity across markets. At the same time, SIFMA has long been extremely concerned and vocal about the protection of CAT Data within the CAT System by the self-regulatory organizations ("SROs") as the developers and operators of the CAT.[4] As we have noted, the value of the data within the system is immeasurable and the SROs have the responsibility to protect it along with

---

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 industry's nearly 1 million employees, 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). For more information, visit http://www.sifma.org.

2 See Release No. 34-89632 (August 21, 2020), 85 FR 65990 (October 16, 2020).

3 Capitalized terms used in this letter have the same meaning as they do in the CAT NMS Plan. For instance, "CAT Data" and "CAT System" are defined in Article I, Section 1.1 of the CAT NMS Plan. CAT Data is defined as "data derived from Participant Data, Industry Member Data, SIP Data, and such other data as the Operating Committee may designate as 'CAT Data' from time to time." CAT System is defined as "all data processing equipment, communications facilities, and other facilities, including equipment, utilized by the [CAT LLC] or any third parties acting on the [CAT LLC's] behalf in connection with operation of the CAT and any related information or relevant systems pursuant to [the CAT LLC Agreement]."

4 See Letter from Kenneth E. Bentsen, Jr., President and CEO, SIFMA, to the Honorable Jay Clayton, Chairman, Commission, dated June 4, 2020 (https://www.sifma.org/wp-content/uploads/2020/06/SIFMA-Letter-on-March-17-2020-CAT-Cybersecurity-Questions.pdf).

the associated liability should the data be exposed. Overall, we believe that the Proposal represents a significant step forward by the Commission in holding the CAT to the highest security standards. We applaud the Commission for issuing it and support much of what is included in it. We nonetheless believe that there are certain minor enhancements, discussed below, that the Commission should consider in connection with finalizing the Proposal.

I. Background

On March 17, 2020, SEC Chairman Jay Clayton issued a public statement in which he announced the release of a Commission order under which broker-dealers would now be required to report to the CAT "phone-book" information regarding retail customers consisting of their names, addresses, and birth years, rather than more sensitive personally identifiable information ("PII") such as their social security numbers ("PII Exemption Order").[5] In addition, Chairman Clayton requested that the Commission staff prepare a recommendation this year for the Commission on improving the data security requirements in the CAT NMS Plan. Chairman Clayton asked the staff to consider seven data security questions related to the CAT in connection with developing the recommendation. These questions addressed, among other things, alternatives to "bulk downloading" CAT Data by each SRO (i.e., the CAT NMS Plan "Participants"), the risks of proliferation of CAT Data across multiple environments, additional data security issues regarding the use of CAT Data for regulatory purposes, oversight of the Plan Processor's security decisions, and additional transparency regarding CAT security and the use of CAT Data without making the CAT System more vulnerable.

On June 4, 2020, SIFMA submitted a letter to the Commission providing our feedback and recommendations on the questions Chairman Clayton posed to the Commission staff.[6] In the letter, SIFMA provided a number of recommendations to improve the security and protection of CAT Data. These recommendations included prohibiting SROs from bulk downloading CAT Data and requiring them to use a Secure Analytical Workspace ("SAW") approach to conduct their surveillance activities, strictly limiting the ability of an SRO to see trading data from other markets, requiring more detail on the permissible regulatory uses of CAT Data by the SROs including the prohibition of the use of such data in connection with rule filings that have a commercial purpose, limiting access to CAT Data to only those SRO employees who need access to it including through the use the use of Role Based Access Control ("RBAC"), adding Industry Member representation to the CAT NMS Plan Security Working Group, and requiring

---

5 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). See also Release No. 34-88393 (March 17, 2020), 85 FR 16152 (March 20, 2020).

6 See supra note 4.

the SROs to notify Industry Members that may have been affected by a security breach of the CAT.

II. Discussion

The Proposal contains many of the recommendations SIFMA and others have made over the years to enhance the security and protection of data within the CAT. The Proposal also incorporates within the Plan the terms of the PII Exemption Order. We therefore are very supportive of the Proposal and encourage the Commission to swiftly adopt it. In doing so, we believe that the Commission should consider adopting additional, minor enhancements related to certain aspects of the Proposal that are described below. We believe that the adoption of these additional enhancements will help to further strengthen the protection of data within the CAT in a manner that is consistent with Commission's goals in issuing the Proposal. We further believe that adopting the Proposal with these additional enhancements will help enhance the overall confidence of the investing public in the CAT, which will hold vast amounts of their data. In our comments below, we highlight first the areas of the Proposal that we believe can be enhanced before briefly addressing the many areas of the Proposal that we support as proposed.

A. Cross-Market Surveillance

In connection with issuing the Proposal, SEC Chairman Clayton and senior Commission staff released an update on the implementation progress of the CAT.[7] In the update, the group acknowledged that one of the outcomes of CAT implementation is the enhanced availability of cross-market order lifecycle data. They noted that this enhancement, as a matter of operational capability, will enable multiple SROs to have access to cross-market data previously unavailable to them. They further stated that the SEC remains receptive to feedback and recommendations on regulatory coordination among the SROs.

SIFMA continues to be very concerned about the ability of exchanges to see the equity and options trading data of other exchanges and Industry Member trading activity that will reside in the CAT. Currently, exchanges only have immediate access to trading activity that occurs within their own exchange group. The current cross-market surveillance responsibilities for the equity and options markets reside almost exclusively at FINRA as a result of the evolution of the for-profit exchange model from member-owned utilities and other market structure changes led individual exchanges to decide over the years to outsource these responsibilities 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

---

[7] See Public Statement by Chairman Jay Clayton, Brett Redfearn, Director, Division or Trading and Markets, and Manisha Kimmel, Senior Policy Advisor, Regulatory Reporting titled "Update on the Consolidated Audit Trail: Data Security and Implementation Progress" dated August 21, 2020 (https://www.sec.gov/news/public-statement/clayton-kimmel-redfearn-nms-cat-2020-08-21).

his speech.[8] 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. Given FINRA's current responsibilities, it is hard to envision scenarios in which one exchange would have a regulatory purpose to see another exchange's trading data.

In addition, as indicated in the CAT implementation update noted above, the current ability of an exchange 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 SRO's regulatory arm through the Intermarket Surveillance Group ("ISG"). 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 without having to go through the hurdle of having to request data from another exchange or FINRA through the ISG. This new paradigm is especially concerning given the for-profit, holding company models followed by most exchanges now and the corresponding continuing pressure they face to drive revenue from new sources. In this regard, SIFMA commends the Commission's decision in the Proposal to explicitly clarify that SROs cannot use CAT Data in connection with a rule filing that has any commercial purpose. As the Commission has recognized, the use of any CAT Data beyond the regulatory purpose for which it was sought or even outside of a regulatory context is a critical security concern for the CAT.

Based on this current regulatory landscape as well as the nonstop pressures exchanges face as for-profit companies, SIFMA believes that it is critically important that the exchanges are clear and transparent on the regulatory scenarios in which they need to see trading data from other markets and that this concept is clearly incorporated into the Plan. SIFMA therefore recommends that the Plan 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. We believe that this exception should be limited only to those situations in which an exchange has a regulatory need to look at the trading data of another market under their rules or the rules of the Commission. For instance, with respect to a qualified contingent trade, an equity exchange may need to view the trading data from an options market to verify that the options leg of the trade was executed as part of confirming that the trade qualified for the exception from the Commission's trade-trough rule (Rule 611 of Regulation NMS).[9] Other than narrow circumstances such as these, an exchange should not have the ability to view the trading data of another market. We similarly believe that exchanges should not have the ability to review the trading data of non-members, as they do not have jurisdiction over them under the Exchange Act, other than in situations in which they have a regulatory need under their

---

[8] 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).

[9] See Release No. 34-57620 (April 4, 2008), 73 FR 19271 (April 9, 2008).

rules or the Commission's rules in connection with their responsibility to surveil their members' activities.

We believe that this concept should be added to the proposed list of requirements in the uniform confidentiality policies and procedures, discussed further below, that all the Participants are required to adopt under the Plan. As noted, the current cross-market surveillance responsibilities for the equity and options markets reside almost exclusively at FINRA and thus only FINRA should be provided with the broad ability to access cross-market CAT Data in the SAW. We believe that placing guardrails on each exchange's access to trading data from other markets is a prudent way for the Commission to address the security concerns related to the ability of SROs to view the trading data of other markets.

We also believe that the adoption and use of monitoring procedures by FINRA CAT regarding an exchange's access to other markets' trading data as well as the logging and tracking of such access would help to further ensure that the data is only used for limited and well-defined regulatory purposes. Moreover, the use of such monitoring by FINRA CAT should serve to further enhance the security of the CAT Data by providing an audit trail of the SROs' access to the data.

In addition, we further suggest that the SEC consider working with the exchanges that do not currently use FINRA for cross-market surveillance activities to encourage them to do so. In addition to addressing potential CAT security concerns, further movement of cross-market surveillance activities to FINRA, coupled with appropriate oversight of costs, should help reduce overall costs to the market of such surveillance as it should eliminate the current duplicative efforts of exchanges in this regard.

B. The PII Exemption Order

SIFMA supports the proposed amendments to modify the Customer-ID creation process and reporting requirements of the Plan consistent with the PII Exemption Order. Specifically, the proposed amendments would no longer require Industry Members to report social security numbers/individual taxpayer identification numbers and account numbers for natural person Customers and would replace the requirement that the date of birth for a natural person Customer be reported with the requirement that the year of birth for a natural person Customer be reported to, and collected by, the CAT.

As part of these amendments, the Commission is proposing that: (1) the defined term "Customer Attributes" replace the defined term "Customer Identifying Information" and the defined term "Account Attributes" replace the defined term "Customer Account Information" to more accurately reflect the data elements being reported by Industry Members; (2) a newly defined term "Customer and Account Attributes" be created to include all the data elements, or attributes, in both "Customer Attributes" and "Account Attributes;" and (3) as a result of the changes to the Customer and Account Attributes that are reported to and collected by the CAT, which will no longer require the reporting of the most sensitive PII, the term "PII" be deleted

from the CAT NMS Plan. In turn, the new term "Customer Attributes" would be defined to include all of the same data elements as "Customer Identifying Information" except the proposed definition would not include the requirement to report ITIN/SSN and date of birth, and the proposed definition would add the requirement that the year of birth for a natural person Customer be reported to CAT. The new term "Account Attributes" would be defined in part to "include, but not [be] limited to, account type, customer type, date account opened, and large trader identifier (if applicable)."

While SIFMA supports these changes, SIFMA has grave concerns that the lack of further clarification by the Commission regarding the terms "customer type" and "account type" in these definitions could be used as an indirect way to impose new recordkeeping obligations on Industry Members. FINRA CAT as the Plan Processor has proposed a list of information, attached as Appendix A, that is expected to be reported to the CAT regarding customer type and account type. This list contains a number of items that may not be able to be readily and systematically reported to the CAT based on the way records are currently maintained by broker-dealers, particularly for long-time customers. For example, the list would require the reporting of whether the customer type is an insurance fund or family office. The list also would require the reporting of whether the account type is a wrap account. This information as well as other information on the list may not be held by a broker-dealer in a format that is readily and systematically reportable to the CAT. Moreover, to require it to be reported to the CAT may require broker-dealers to make extensive and costly system changes.

Such an outcome would clearly conflict with the Commission's expressed view in the release adopting Rule 613 of Regulation NMS that the CAT is not intended to impose new recordkeeping obligations on broker-dealers.[10] Moreover, this type of information is well beyond what is needed to identify a customer to a trade across markets and broker-dealers, which is the primary purpose of the CAT. SIFMA therefore requests that the Commission clarify that the scope of the terms "customer type" and "account type" are strictly bounded by the existing recordkeeping obligations and that the information that Industry Members would be required to report regarding customers and their accounts is the information (i) that firms are already required to maintain under existing recordkeeping obligations and (ii) that is capable of being readily and systematically reported to the CAT. Moreover, such an approach would be consistent with the security concerns expressed by the Commission in issuing the Proposal, which is intended to limit the amount of customer and account data maintained in the CAT.

Similarly, SIFMA is concerned about the reporting to the CAT of certain information regarding "[a]ny person from whom the broker-dealer is authorized to accept trading instructions for such account, if different from the account holder(s)." Such persons ("Authorized Traders") are defined as "customers" under Rule 613, and the CAT NMS Plan contemplates that firms

---

[10] For example, the Commission stated in the release that "Rule 613 is not intended to alter in any way the information that a broker-dealer is currently required to obtain under Rule 17a-3(a)(9)." See Release No. 34-67457 (July 18, 2012), 77 FR 45721 (August 1, 2012). Rule 17a-3(a)(9), among other things, requires a broker-dealer to make and keep a record of the name and address of the "beneficial owner" of each cash or margin account with the broker-dealer.

would have certain information on such persons that would allow them to be tracked across broker-dealers in the CAT. In particular, the Plan contemplates that for natural persons serving as Authorized Traders, broker-dealers would have the social security numbers of such individuals, which in turn would be converted through the CCID process to a unique identification that will allow the tracking of such individuals across broker dealers in the CAT. The issue with this approach is that broker-dealers are not required to maintain the social security numbers of non-associated persons under existing recordkeeping requirements. SIFMA therefore requests that the Commission direct the Participants and FINRA CAT to work with Industry Members to develop a workable approach regarding the reporting of information with respect to Authorized Traders. Such an effort would be consistent with the Commission's overall approach in the Proposal to reduce the amount of sensitive information held in the CAT.

Finally, SIFMA questions the Commission decision to delete the term PII in the CAT NMS Plan. While we recognize that the most sensitive customer information will no longer be required to reported to the CAT by Industry Members, the CAT will continue to hold PII regarding customers such as their names and addresses. It therefore seems that there is a continuing need to maintain the PII definition in the Plan to be able to differentiate the customer information that will continue to be held in CAT and to potentially apply heightened obligations regarding the use of such data.

C. The SAWs

The Proposal would require FINRA CAT as the Plan Processor to create the SAWs, direct Participants to use the SAWs to access and analyze CAT Data obtained through their user-defined direct query and bulk extract tools (i.e., surveillance queries) and any customer and account data, set forth requirements for the data extraction, security, implementation, and operational controls that will apply to the SAWs, and provide an exception process that will enable Participants to conduct their surveillance queries with regard to transaction data in other environments subject to security controls consistent with the ones for the SAWs. The Proposal would further provide that Participants may only extract from SAWs the minimum amount of CAT Data necessary to achieve a specific surveillance or regulatory purpose.

As noted, the Proposal sets forth a process by which Participants may be granted an exception from using the SAW to review transaction data from the CAT in their own environment. The Proposal would continue to require Participants to access and review any customer and account data in the SAW. Specifically, the Proposal would require the Participant requesting an exception to provide the Plan Processor's CISO, the CCO, the members of the Security Working Group (and their designees), and Commission observers of the Security Working Group with various application materials ("Exception Application Group"), including a security assessment of the non-SAW environment, conducted within the prior twelve months by a named, independent third party security assessor, that among other things demonstrates the extent to which the non-SAW environment complies with the NIST SP 800-53 security controls. Under the Proposal, the CCO and CISO may jointly grant the exception if they determine, in accordance with policies and procedures developed by FINRA CAT as the Plan Processor, that

the residual risks identified in the security assessment or detailed design specifications provided by the requesting Participant do not exceed the risk tolerance levels set forth in the risk management strategy developed by the Plan Processor for the CAT System pursuant to NIST SP 800-53. In discussing this proposed exception, the Commission notes that FINRA and a few other SROs have already developed cloud-based surveillance capabilities that may not be able to be transferred over to the SAW in an efficient and cost-effective manner.

SIFMA supports the Commission's proposed amendments regarding the SAWs but believes that they can be further enhanced to protect CAT Data. While SIFMA continues to believe that all of the SROs' surveillance activities should be conducted in the SAWs "to minimize the attack surface associated with CAT Data,"[11] SIFMA acknowledges the Commission's decision to provide an exception from the mandated use of the SAWs for the review of transaction data for those SROs that already employ cloud-based surveillance functionality. SIFMA particularly supports the Commission's decision in connection with the proposed exception to continue to require that customer and account data only be viewed in the SAW.

Nevertheless, to ensure that the exception is appropriately limited in a manner that is designed to foster the protection of CAT Data, SIFMA recommends that the Commission require any Participant seeking such an exception to provide to the Exception Application Group noted above a description of the surveillance activities that they plan to conduct with the downloaded transaction data in its application. We further recommend that the Commission as an independent (i.e., non-SRO), expert party interested in the security of CAT Data either formally approve, or not-object to, the granting of such an exception. These additional steps would help ensure that the exception is appropriately limited to legitimate regulatory uses as opposed to allowing an SRO to seek an exception just because it can without having to clearly demonstrate what it intends to do with the downloaded transaction data from the CAT. It also would help ensure that exchanges are not downloading the transaction data of other markets outside of the monitored SAW environment such that they could use the data outside of limited regulatory purposes for which it was sought, consistent with our concerns expressed above with regard to cross-market surveillance. Moreover, involving the Commission in this process would be designed to ensure that CAT Data security is a paramount consideration, as any grant of such an exception would increase the number of environments in which the CAT Data resides and thus increase the risk of its exposure.

D. Security Working Group

The Proposal would require the establishment of a permanent Security Working Group that will be composed of the CAT's Chief Information Security Officer ("CAT CISO"), and the chief information security officer or deputy chief information security officer of each SRO that is a Participant to the CAT NMS Plan. The Proposal would provide that Commission observers

---

[11] See Proposal at 65995.

can attend the working group's meetings and that the CAT CISO and the Operating Committee may invite other parties to attend specific meetings.

The Security Working Group's purpose will be to advise the CAT CISO (who in turn reports directly report to the Operating Committee in accordance with the Plan) and the Operating Committee, including with respect to issues involving: (i) information technology matters that pertain to the development of the CAT System; (ii) the development, maintenance, and application of the Comprehensive Information Security Program; (iii) the review and application of the confidentiality policies and procedures required by the Plan; (iv) the review and analysis of third party risk assessments conducted pursuant to the Plan, including the review and analysis of results and corrective actions arising from such assessments; and (v) emerging cybersecurity topics.

SIFMA applauds the Commission's decision to make the Security Working Group permanent. Industry Members and other industry representatives currently participate on a CAT Advisory Committee that provides the Participants 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. In addition, SIFMA member firms and other industry representatives, including the CAT Advisory Committee are generally precluded from participating in the Security Working Group meetings.

SIFMA believes that the Security Working Group could greatly benefit from the permanent inclusion of industry representatives with voting rights in the group. SIFMA continues to believe that a working group with industry input could help enhance the security of the CAT by providing "best-practice" advice to the Plan Processor and Operating Committee regarding security practices that work well at the non-SRO organizations represented on the working group.[12] In turn, it could also serve as a security resource to all of the organizations represented on the working group. As it stands today, however, industry representatives are not included on the Security Working Group and thus have very little insight into the level of engagement the working group has with respect to CAT security. This is unfortunate given the significant level of expertise Industry Members and other market participants have in protecting customer data. SIFMA therefore believes that Industry Member representation should be added to the Security Working Group, which could help enhance its effectiveness much like the work SRO and SIFMA member representatives conducted to find a solution for collecting PII data that is reflected in the PII Exemption Order.

To the extent there are concerns about adding Industry Member representatives to the Security Working Group, SIFMA believes that these concerns are misplaced. Industry Members have just as much interest in protecting the CAT Data as SROs do, so there is significant high-level alignment of the firms and SROs' security interest in protecting the CAT Data. In addition, as noted, Industry Members have tremendous experience in protecting customer data and can

[12] See supra note 4.

serve as a valuable resource in this regard. Moreover, the data in the CAT System is ultimately the Industry Members' data. To the extent the SROs are concerned about discussing certain regulatory issues with industry representatives, the Plan could specify the processes that the SROs follow to ensure that Industry Member participation in the group will be limited to only enhancing the security posture of the CAT. Finally, it is worth noting that the likely participants from the Industry Members will already have high-level government security clearances and would sign non-disclosure agreements to limit their ability to discuss Security Working Group matters outside of the group, much as they did in connection with SIFMA's engagement in the solution presented in the PII Exemption Order.

E. Participants' Data Confidentiality Policies and Procedures

The proposal would require the SRO Participants to adopt and maintain identical written data confidentiality policies. In turn, each Participant would establish and maintain procedures and usage restrictions in accordance with these policies. In addition, the Participants would be required to make the data confidentiality policies publicly available on a website, and on an annual basis each Participant would be required to engage an independent accountant to perform an examination of compliance with the data confidentiality policies.

The Proposal also would define the term "Regulatory Staff" of the SROs and the data confidentiality policies adopted by Participants would be required to limit access to CAT Data to Regulatory Staff, and certain technology and operations staff, except when there is a specific regulatory need and a Participant's Chief Regulatory Officer (or similarly designated head(s) of regulation), or his or her designee, documents written approval to provide such access. The policies would also limit the extraction of CAT Data, define the roles and regulatory activities of specific users, and require implementation of the Customer Identifying Systems workflow along with supporting requirements for monitoring and testing. Further, the Proposal would also require that CAT Data be accessed only for surveillance and regulatory purposes and forbid the use of CAT Data where such use may serve both a surveillance or regulatory purpose, and a commercial purpose (e.g., economic analyses or market structure analyses in support of rule filings).

SIFMA strongly supports these amendments, and particularly the limitation on the ability of non-Regulatory Staff to view CAT Data as well as the explicit prohibition on the use of CAT Data in connection SRO commercial endeavors such as rule filings that serve both a regulatory and commercial purpose. We have long been concerned about the general ability of SRO staff to view CAT Data and believe that the Commission's approach strikes the right balance here. Similarly, we are grateful for the explicit inclusion of the limit on the ability of SROs to use CAT Data in connection with rule filings that serve any commercial purpose, as this has been a SIFMA concern for some time.

In addition to the inclusion of the limits on the ability of one exchange to see the trading data of other markets discussed in the Cross-Market Surveillance section above, we believe that the data confidentiality policies could be enhanced by subjecting them to a public notice and

comment period. Such a process would allow the policies to be subject to public input from investors and securities industry participants whose data will reside in the CAT System. Given the materiality of the policies, the Commission could subject them to a public comment process either through the SRO rule filing process under Section 19(b)(1) of the Exchange Act or as an amendment to the CAT NMS Plan.

F. Other Aspects of the Proposal

SIFMA strongly supports the other proposed amendments to the CAT NMS Plan that are included in the Proposal. For instance, SIFMA supports the proposed amendments to the Plan that more clearly describe the "Comprehensive Information Security Program" that the Plan Processor is required to adopt. The proposed amendments would more explicitly delineate the coverage of the overarching security framework that FINRA CAT is required to adopt and maintain pursuant to the Plan. Similarly, SIFMA supports the proposed amendments to the Plan that would limit the maximum amount of records that regulators can download using an online targeted query tool and would enhance the CAT logging requirements by requiring logging of extraction of CAT Data. Both of these proposed amendments are designed to further enhance the security of CAT Data by limiting the ability of Participants to use the online targeted query tool to evade the SAW usage requirements and by further tracking the extraction of CAT Data by Participants. SIFMA also supports the proposed amendments to the Plan to explicitly require that corrective actions and breach notifications to CAT Reporters be part of the Plan Processor's cyber incident response plan. These changes are modeled after the SROs' Regulation SCI obligations and have long been supported by SIFMA as they would allow Industry Members to react more quickly to CAT breaches that may involve the firms' data.

Similarly, SIFMA supports the proposed amendments to define the workflow for accessing customer and account attributes and to establish restrictions governing such access. In particular, Customer Identifying Systems, which contain customer and account attributes, would be required to be accessed through a Participant's SAW. In addition, only Regulatory Staff may access Customer Identifying Systems and such access would have to follow RBAC and the "least privileged" practice of limiting access to Customer Identifying Systems and customer and account attributes as much as possible. We further believe that the Plan should explicitly provide, like our comment above on cross-market surveillance, that exchanges' access to customer and account data should be limited only to those circumstances in which an exchange needs access to that data under its rules or the rules of the Commission. This additional requirement is designed to help further protect access to customer and account data.

* * *

SIFMA greatly appreciates the Commission's consideration of our comments above and would be pleased to discuss them in greater detail. As noted, we are very supportive of the Proposal and encourage the Commission to swiftly adopt it. In so doing, we believe that the Commission should consider adopting additional, minor enhancements related to certain aspects

of the Proposal that are described above and that we believe will help to further strengthen the Proposal in a manner that is consistent with Commission's goals in issuing it. If you have any questions or need any additional information, please contact me at 212-313-1287 or egreene@sifma.org.

Sincerely,

Ellen Greene

Ellen Greene
Managing Director
Equity and Options Market Structure

cc: The Honorable Jay Clayton, 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

Brett Redfearn, Director, Division of Trading and Markets
Manisha Kimmel, Senior Policy Advisor for Regulatory Reporting

Appendix A

Consolidated Audit Trail

Customer and Account Information System (CAIS)

Inconsistency Management

Presented by FINRA CAT on October 22, 2020

Agenda

- Account and Customer Type Values
- Inconsistencies
  - Plan Requirements
  - Principles
  - Framework
  - Resolution Procedures

Account Types

Proposed Account Types include the following Boolean attributes:

- Is Retirement – Including Pension Plans, Roth IRA, IRA, 401(K), 403(b), ERISA accounts, etc
- Is Managed – Indicates CAT Customer has authorized another entity to trade on the account without prior customer approval
- Is Online/Direct – Is the account set up for self-directed trading
- Is Approved for Margin
- Is Approved for Options Trading
- Is Wrap – Is an investment account where the customer is charged a single bundled, or 'wrapped', fee for investment advice, brokerage services, administrative expenses, and other fees and expenses typically based on assets under management
- Is Education – Is a 529 Plan or Coverdale ESA
- Is UGMA/UTMA
- Is DVP/RVP
- Is Firm Account – Including proprietary trading accounts and inventory accounts
- Is Market Making
- Is Average Price Account
- Is Error Account

1. *Do these values present challenges for Reporters to provide?*
2. *Are the definitions consistent with how the industry defines these terms?*

4

Customer Types

Proposed Customer Types include the following Boolean attributes:

- Is Natural Person
- Is Trust
- Is Non-Profit
- Is Private Fund
- Is Registered Investment Company/Business Development Company
- Is Insurance Fund
- Is Family Office
- Is Accredited Investor
- Is Qualified Purchaser
- Is Affiliated with a Broker
- Is Affiliated with an Investment Advisor
- Is Foreign
- Is Broker/Dealer
- Is Bank
- Is Officer or Director of Public Company
- Is Sole Proprietor

3. *Do these values present challenges for Reporters to provide?*
4. *The CAT NMS Plan requirements consider Customer Type an Account attribute. Is this data stored on the Account or Customer record at the firms?*

5